Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Study on Cyber Security and Threat Evaluation in SCADA Systems

Marc Fabro

Lofty Perch, Inc.

Scientific Authority: Rodney Howes
DRDC Centre for Security Science

Defence R&D Canada – CSS
Contract Report
DRDC CSS CR 2012-006
March 2012

Canada

Study on Cyber Security and Threat Evaluation in SCADA Systems

Marc Fabro

Lofty Perch, Inc.
15-505 Hood Road
Markham, ON
L3R 5V6

Scientific Authority: Rodney Howes,
DRDC Centre for Security Science

Defence R&D Canada – CSS

Contract Report
DRDC CSS CR 2012-006
March 2012

Principal Author

Original signed by Marc Fabro

Marc Fabro

Lofty Perch

Approved by

Original signed by Rodney Howes

Rodney Howes

DRDC Centre for Security Science

Approved for release by

Original signed by Dr. Mark Williamson

Dr. Mark Williamson

DRDC Centre for Security Science, DRP Chair

PSTP 02-347eSec

Abstract

This report summarizes the finding of study PSTP 02-0347eSec Study on cyber Security and Threat Evaluation in SCADA Systems. The primary objective of the study was to support the e-Security Community of Practice by leading a study to fill the knowledge gap concerning the current cyber-threat environment affecting SCADA systems. This work is intended to enhance the resilience of Canada's critical infrastructure by providing direction to research and development programs and recommending best security practices. This primary objective is supported by the following complementary objectives:

1. To establish trusted relationships with private sector critical infrastructure SCADA operators;
2. To enable the production of research reports on the current cyber-threat environment to SCADA systems;
3. To contribute to the development of a cyber-threat management system for continued situational awareness; and
4. To contribute to the development of best practices for the security of SCADA systems.

The report is divided into five parts :

1. Task 1 Milestone “Assess State of the Art for SCADA Security”
2. Task 2 Milestone “Development of a Cyber Threat and Vulnerability Guideline”
3. Task 3 Milestone “Define the Scope and Capabilities of a Cyber-Threat and Vulnerability Management System”
4. Task 4 Milestone “Produce a Best Practices Security Manual or Guide”
5. Final conclusions, strategic advisory note, capabilities road map, study fact sheet, and quad chart

Résumé

Le présent rapport fait la synthèse des résultats du projet PTSP 02-0347eSec intitulé Étude en cybersécurité et en évaluation des menaces pour les systèmes SCADA. L'objectif principal des responsables du projet est d'appuyer la communauté de praticiens de la sécurité électronique par la réalisation d'une étude scientifique qui vise à combler les lacunes dans les connaissances sur l'environnement de cybermenace actuel qui affecte les systèmes d'acquisition et de contrôle des données (SCADA). Ces travaux ont pour but d'accroître la résilience des infrastructures essentielles canadiennes en fournissant une orientation aux programmes de recherche et de développement et en recommandant des pratiques exemplaires en matière de sécurité. Cet objectif principal se divise en objectifs complémentaires de la façon suivante :

1. établir des relations de confiance avec les opérateurs SCADA des infrastructures essentielles du secteur privé;
2. permettre la production de rapports de recherche sur l'environnement de cybermenace actuel qui affecte les systèmes SCADA;
3. contribué à l'élaboration d'un système de gestion des cybermenaces qui favorise une connaissance constante de la situation;
4. contribuer à l'élaboration de pratiques exemplaires pour la sécurité des systèmes SCADA.

Le rapport se divise cinq parties :

1. Tâche 1 : « Évaluer ce qui se fait de mieux en matière de cybersécurité des systèmes SCADA »
2. Tâche 2 : « Élaboration de lignes directrices en matière d'évaluation de la cybermenace et de la vulnérabilité »
3. Tâche 3 : « Définir la portée et les capacités d'un système de gestion de la cybermenace et de la vulnérabilité »
4. Tâche 4 : « Rédiger un guide ou un manuel des pratiques exemplaires en matière de sécurité »
5. Conclusions finales, note de consultation stratégique, feuille de route des capacités, fiche d'information relative à l'étude et tableau à quatre volets

Executive summary

Study on Cyber Security and Threat Evaluation in SCADA Systems:

Marc Fabro; DRDC CSS CR 2012-06; Defence R&D Canada – CSS; March 2012.

This report details the methodology, research, findings, conclusions and recommendations of Study on Cyber Security and Threat Evaluation in SCADA Systems. The document provides a report on specific tasking as it pertains to the 'Final Study Report, Capability Roadmap, Final Quad Chart and Project Fact Sheet'. This document provides material summarizing content developed from a comprehensive review of the reporting across all study tasks. It includes other project completion activities including strategic advisory guidance, capability roadmap, a project fact sheet and a final quad chart for review purposes.

Overall, the study was completed on time and met or exceeded all expectations as defined by study objectives. In addition, due to the experience of the study leadership and their access to technology and industry stakeholders, the study was completed under budget. As the study was performed concurrent with many real-world SCADA security projects being performed by the study research team, additional observations and findings were able to enhance the work done in a laboratory environment.

The study results and recommendations were as follows:

- PSTP study programs that include dedicated activities towards a better understanding of SCADA and control system cyber security have tremendous value to Canadian critical infrastructure asset owners
- The SCADA security technical capabilities and subject matter expertise within the Canadian community of interest is considerable, the current level of interest demonstrated by the federal government is well-positioned to accommodate current and future requirements to leverage this expertise in infrastructure resiliency programs
- Existing commercial security technologies have applicability in SCADA security programs, and those technologies addressing intrusion detection/prevention and forensics can clearly improve defensive strategies when deployed with due care. In many cases, the somewhat standard network configurations of SCADA networks creates opportunities for straightforward defensive strategies applicable across many sectors, and modifications in traditional deployment configurations can greatly improve the protection of control system domains.
- The volume of SCADA security research and information that is available from the global community is substantial, and the ubiquitous problem of how to secure control systems allows this information to have widespread and significant positive impact on the security risk profiles of Canadian critical infrastructure.
- Existing frameworks used by public and private sector entities to manage cyber threats and vulnerabilities are well-suited to accommodate for the requirements

associated with SCADA systems. In addition, elements derived from historical approaches to threat and vulnerability management can be updated to create the capabilities to meet future states of threat management requirements.

- The effective deployment of security countermeasures within industrial control system environments is often dependent upon asset owner's willingness and technical expertise to customize commercial security technologies. However, those stakeholders that have created SCADA security risk reduction programs can provide insight that enhances current resiliency strategies and may be better prepared for information sharing with law enforcement and intelligence entities.

- The number of vulnerabilities that are specific to SCADA vendor technology is increasing, as is the understanding of research strategies and the inclusion of these vulnerabilities into contemporary exploit frameworks. In addition, the security of SCADA systems is also significantly impacted by vulnerabilities that are unique to underlying operating systems or third-party applications (as opposed to specific SCADA vendor solutions).

- The number of standards and recommended practices specific to SCADA security has increased considerably in the recent year, as has the amount of usable guidance uniquely designed for individual critical infrastructure sectors

Sommaire

Étude en cybersécurité et en évaluation des menaces pour les systèmes SCADA.

Marc Fabro ; DRDC CSS CR 2012-006 ; R & D pour la défense Canada – CSS; mars 2012.

Le présent rapport décrit la méthodologie, les recherches, les résultats, les conclusions et les recommandations de l'Étude en cybersécurité et en évaluation des menaces pour les systèmes SCADA. Il fait état d'une la tâche particulière du projet, soit la production du rapport d'étude final, de la feuille de route des capacités, du tableau final à quatre volets et de la fiche d'information. Il fait la synthèse du contenu élaboré à partir d'un examen approfondi des rapports produits par l'ensemble des tâches liées à l'étude. Le rapport couvre d'autres activités liées à la réalisation du projet, dont un guide contenant des conseils stratégiques, une feuille de route des capacités, une fiche d'information sur le projet et un tableau final à quatre volets aux fins d'examen.

Dans l'ensemble, l'étude réalisée dans les délais impartis a répondu aux attentes fixées dans les objectifs de l'étude, voire dépassé celles-ci. En outre, les limites du budget alloué ont été respectées grâce à l'expérience des dirigeants de l'étude et aux relations qu'ils entretiennent avec les intervenants de l'industrie et du domaine de la technologie. L'étude ayant été réalisée parallèlement à d'autres projets concrets sur la sécurité des systèmes SCADA dont était chargée l'équipe de recherche, d'autres résultats et observations ont permis de rendre plus efficace le travail accompli en laboratoire.

Voici les résultats de l'étude et les recommandations qui en découlent :

- Programmes de l'étude du PTSP comprenant des activités qui visent à mieux comprendre la cybersécurité des systèmes SCADA et des systèmes de contrôle présentant une importance capitale aux yeux des propriétaires de biens d'infrastructure essentielle au Canada.

- Les capacités techniques en matière de sécurité des systèmes SCADA et l'expertise de la communauté d'intérêts canadienne sont considérables. Le gouvernement fédéral manifeste présentement un tel intérêt qu'il mettra à profit cette expertise en matière de programmes touchant la résilience de l'infrastructure en regard des besoins actuels et à venir.

- Les technologies de sécurité disponibles sur le marché peuvent s'appliquer aux programmes de sécurité des systèmes SCADA, et celles qui ont trait à la détection/prévention des intrusions et à la recherche de preuves améliorent nettement les stratégies de défense lorsqu'elles sont mises en œuvre avec la prudence nécessaire. Dans bien des cas, les configurations plus ou moins normalisées des réseaux SCADA favorisent la mise en place de stratégies de défense simples dans de nombreux secteurs, et les changements apportés aux configurations de déploiement habituelles peuvent fortement améliorer la protection des systèmes de contrôle.

- La communauté mondiale propose une quantité considérable d'ouvrages de recherche et de documents sur la sécurité des systèmes SCADA. La protection des systèmes de contrôle étant un problème omniprésent, cette masse d'information se répercute de façon positive et généralisée sur le profil des risques liés à la sécurité de l'infrastructure essentielle du Canada.

- Les cadres de gestion des cybermenaces et des vulnérabilités dont se servent aujourd'hui les entités des secteurs public et privé sont bien adaptés aux exigences ayant trait la sécurité des systèmes SCADA. De plus, des éléments tirés des approches adoptées dans le passé dans ce type de gestion peuvent être actualisés de manière à créer les capacités nécessaires pour répondre aux besoins futurs dans ce domaine.

- Le déploiement efficace de contre-mesures de sécurité à l'intérieur d'un environnement informatique de contrôle est souvent tributaire de la volonté du propriétaire du bien d'acquérir des programmes de sécurité commerciaux et de son expertise technique qui lui permettrait d'adapter ceux-ci à ses besoins particuliers. En revanche, les intervenants à l'origine de tels programmes de réduction des risques liés à la sécurité des systèmes SCADA peuvent communiquer leurs idées et améliorer ainsi les stratégies de résilience actuelles. Ils seraient également mieux placés pour échanger l'information avec les organismes chargés d'appliquer la loi et ceux du renseignement.

- Le nombre de vulnérabilités particulières à la technologie des systèmes SCADA ne cesse d'augmenter, tout comme l'on comprend mieux les stratégies de recherche et l'inclusion de ces vulnérabilités dans les cadres d'exploitation modernes. Également, la sécurité des systèmes SCADA est sérieusement compromise par les vulnérabilités que présentent les systèmes d'exploitation sous-jacents ou les applications de tierce partie (par opposition aux solutions du fournisseur SCADA).

- Les normes et les pratiques recommandées qui ont exclusivement trait aux systèmes SCADA se sont considérablement multipliées depuis quelques années, et le volume de conseils pratiques destinés à chacun des secteurs de l'infrastructure essentielle à lui aussi explosé.

Table of contents

Acknowledgements

Lofty Perch recognizes the extensive support it received from its in-kind partners during the tasking activities, and in the final report deliverable will (wherever possible) be citing them by name. During the development of this and other report content it was deemed necessary to withhold the identity of partners due to the sensitive nature of the observations and findings. Lofty Perch has, to the best of its ability, developed the material in this report to empower the reader to select the most appropriate technologies for their security needs. In addition, the material is delivered in a manner that can facilitate for useful discussions between researchers and vendors, and provide valuable perspectives on current capabilities and future needs.

This work was supported by DRDC Centre for Security Science under study PSTP 02-347eSec and partners in RCMP, National Security Criminal Investigations.

This page intentionally left blank.

1 Introduction – Task 1- Assess State of the Art for SCADA Security

This document provides a comprehensive report on specific tasking as it pertains to Project Task 1 - Assess State of the Art for SCADA Security. The tasking in this project area was comprised of three core activities, all of which were performed with the study's primary and supporting objectives in mind: Evaluate existing security technologies in view of identifying the best solutions for capturing wired and wireless SCADA traffic and detecting malicious activity.

Identify the capability gaps in efficiently detecting malicious traffic targeting SCADA systems, and survey and evaluate the research literature in relation to work being done to improve this capability.

Evaluate forensic technologies and techniques that can be leveraged to understand the response of SCADA systems to malicious traffic.

Lofty Perch, Inc. (LPI) and the study team performed extensive research during this study activity, and in addition to working on other study areas concurrently, LPI executed lab and field based testing in collaboration with industry stakeholders and in-kind partners. LPI made significant findings regarding communications capture techniques in SCADA and control system domains, and cross-correlated their findings with study work on intrusion detection and intrusion prevention capabilities. Perhaps most interesting is the fact that during the actual work activities LPI was involved in two (2) cyber-security incidents and seven (7) security assessments involving industrial control systems[1]. Using their on-site experience, the study team was able to make significant contributions to the study's requirements involving the evaluation of security technologies and techniques applicable to SCADA and industrial automation. The integration of findings from the resultant field work allowed for direct investigation pertinent to specific study tasking areas while actively supporting the study's primary and complementary objectives.

The sub-tasking for the evaluation of existing security technologies that capture wired and wireless traffic to detect malicious activity on a control system network indicates that current commercial-off-the-shelf (COTS) and open-source network analysis tools are adequate for performing traffic analysis. However, current technology is best suited for network based communications, and there are a number of technical capability requirements that vary depending on the complexity of the architecture. Although existing traffic analysis technologies are suitable for non-routed protocols, the study has shown that the most effective capabilities exist when analysis is being performed in a networking environment.

The detection of malicious traffic is dependent on tuning the technology to either look for deviations in normal communications behaviour or to incorporate known intrusion signatures into the analysis. The study shows that technology designed to detect malicious traffic, or more accurately technology that can be tuned for SCADA environments, can only be optimized fully when administered by a subject matter expert. To that end, the subject matter expertise required to optimize malicious traffic detection capabilities should be specific to the control system domain and, perhaps more importantly, specific to the actual control system technology and communication protocol. This observation suggests that future strategies for defending against malicious activity in SCADA networks will an active collaboration between the IT security, engineering, and vendor domains.

[1] These activities were performed on both wired and wireless systems, and facilitated for extensive real-world observation and collaboration with asset owners.

The study team performed a comprehensive review of existing literature regarding historical perspectives on the functional requirements for detecting and mitigating abnormal and possibly malicious traffic targeting SCADA systems. During this review, a contrast and compare of historical and current/future trending was performed, and it was observed that a significant amount of academic and independent research provides a foundation for future technology development. It was also noted that several government research and development projects have resulted in technology specific for traffic analysis and intrusion detection for control systems, and that some of this technology is being transferred into the private sector domain. The rate at which this technology is being developed and deployed is concurrent with the growing security needs asset owners are experiencing. From this, it may be concluded that the gap between contemporary intrusion detection requirements and intrusion detection requirements for SCADA systems is closing, but more work is required.

This initial task also focused on the evaluation of forensic technologies and techniques that can be used in responding to SCADA system security events and analyzing malicious traffic. As mentioned above, during the study period the research team was engaged in two incident response engagements that directly involved the application of contemporary forensic investigation techniques and technologies, while simultaneously supporting investigations using current best practices and guidance. The observations and analysis from this activity has resulted in an improved understanding of current forensic computing approaches as applied to SCADA systems, and has uncovered some existing gaps in both techniques and technologies required to perform comprehensive investigations on industrial automation.

Concurrent to these field investigations, the study team worked closely with in-kind partners to perform analysis of commercial forensic technologies and determine if and how they can accommodate the unique operational environments associated with SCADA systems. This activity also coincided with regular interactions with several national law enforcement and intelligence entities, resulting in a substantial set of conclusions that have proven useful in other study task areas.[2]

This document is intended to provide content to be used in the comprehensive material to be delivered in the Final Project Study Report. The material in this document will, where possible, reference other study activities so that the reader will be able to interpret and leverage the information efficiently.

Section 2 is dedicated to discussing tasking and sub tasking activities, with in-depth discussion about the process, procedures, and investigative models used during the tasking. Section 3 discusses the findings and observations from the study activities, and from the analysis of how current state-of-the-art cyber-security technology and techniques may be applied to protecting SCADA and industrial control systems. Section 4 discusses conclusions, followed by appendices providing project workflow, literature sources, and an introduction to the base questions used in collecting traffic analysis requirements from critical infrastructure asset owners.

1.1 Description of tasking and sub- tasking activities

The primary task element, as a function of the overall study methodology, is shown in figure 2 below. This is derived from the comprehensive Study Workflow as shown in Appendix A.

[2] As RCMP is the Technical Authority for the project, and subsequent study tasking addresses law enforcement stakeholder requirements, Lofty Perch found the investigation activities and results pertinent to other areas in the study program. These findings and observations will be represented in other tasking reports in addition to this one.

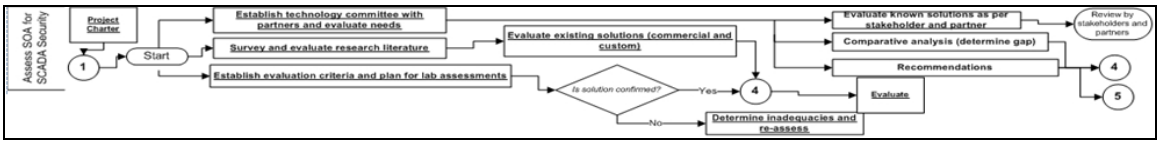


Figure 2 - Detailed workflow for Task 1

The core activities of this task involved the establishment of the technical committee with partners, advisors, and subject matter experts specifically interested in addressing issues related to the detection and mitigation of malicious traffic in SCADA and control system environments. As this was the initial tasking activity for the study, the team study team leveraged their access to the asset owner, vendor, and research community to harvest current best practices and methodologies used. This approach provided foundations for the study team to understand what proven technical capabilities exist that are being used in real-world SCADA deployments.

In addition, concurrent research involving the testing and analysis of commercial technologies in the Lofty Perch laboratory created mechanisms to compare observations in real-world SCADA deployments against those obtained in a test environment. To facilitate this research, the study team used the real control system environment developed for the Lofty Perch intermediate and advanced training. This system comprises a variety of technical capabilities that include PLCs, field equipment, operator workstations, human machine interfaces, primary application servers and other capabilities that can be tuned to create a system mock-up for almost any architecture required. This proved exceptionally useful in the development of the architecture types developed for the first subtask in this activity. The study team also ensured that their approach took into consideration interoperability and interdependencies of both wired and wireless networks, and leveraged their technical subject matter expertise to create laboratory environments that addressed both technologies. The skill set required for the acquisition, configuration and deployment of commercial traffic capture technologies, both wired and wireless, was consistent with the level of expertise available in the network and engineering departments of more sophisticated asset owners.

The assessment tasking required the development of two very different approaches. By leveraging access to the vendor community, as well as the critical infrastructure asset owner community, the study team was able to ascertain that the technology requirements related to capturing and evaluating control system traffic (with the intent to look for abnormal behaviour which could be malicious) and the technology related to performing forensics investigation are quite different. Tasking in the study directed the research to evaluate forensic technologies and techniques that can be used to understand the response of SCADA systems to malicious traffic. The study team felt that investigating forensic technologies and techniques that can be used both during and *after* an abnormal cyber-incident would provide additional value to the primary task. This approach yielded both expected and unexpected results, and provided for a set of observations and analysis that will have a significant contribution to the final report and, more importantly, the material presented in the Best Practices Security Manual for Canada's critical infrastructure owners (Study Task 4).

Task 1 was completed using a series of core activities:

Establishment of interim technical committee

Perform a literature review on current and emerging theoretical strategies involving intrusion detection and anomaly detection in SCADA and industrial control system environments, and begin to map those findings against the observations from laboratory research

Interaction with private sector asset owners to survey mission critical SCADA firmware and over-the-air (OTA) upgrade capabilities

Modification of the Lofty Perch proprietary assessment framework to allow for customization based on available in-kind support from asset owners and vendor community

Development and deployment of lab-based SCADA radio system, and comparative analysis of security functionality and requirements of collateral wireless communications

Build-out of commercially available wired and wireless network protocol analyzers and deployment of these analyzers in both laboratory and field environments
Detailed discussion with SCADA and security vendor community representation regarding current and emerging capabilities for traffic analysis in both wired and wireless architectures
Configure and customize traffic generating technology for specific SCADA and industrial control system environments, and use partner technology to create a broad range of malicious stress and duress scenarios
Obtain, configure, and test several commercially available anomaly and intrusion detection systems for applicability and usability in control system environments
Obtain, configure, and test perimeter-level defensive technologies designed specifically for industrial automation equipment and architectures
Obtain and configure market-leading forensic technology and perform forensics analysis on impacted SCADA and control architecture elements in both a proactive and reactive manner
Commence in-house analysis of emerging SIEM algorithm-based anomaly detection capabilities, and contrast/compare against current market leading signature-based solutions
Test applicability of various commercial forensics technologies on actual SCADA systems, and in particular evaluate feasibility of post-incident memory analysis against feasibility of live memory analysis using active servlets and application state monitoring
Revisit contemporary best practices as published by the US Department of Homeland Security and review feasibility of proposed identification models used in the development of forensic investigation methods for SCADA systems
Engage representation from the law enforcement community to obtain perspectives related to advantages and disadvantages in various approaches involving forensic analysis on industrial automation
Engage representation from the asset owner community to obtain perspectives on acceptance or reticence related to the employment of forensic computing strategies within the industrial control system domain
Leverage access to the research community to discuss emerging strategies regarding forensics in SCADA, and leverage physical presence at many SCADA security conferences (globally) to facilitate discussions on academic and asset owner perspectives on requirements for forensic capabilities in sector specific environments

Approach to Subtask 1.1: Evaluate existing security technologies in view of identifying the best solutions for capturing wired and wireless SCADA traffic and detecting malicious activity.
Lofty Perch modified their proprietary target of evaluation criteria for the laboratory assessments and performed numerous interview engagements with Canadian critical infrastructure asset owners. From these interviews and interactions, the study team was able to assess the needs and requirements that were often customized to a sector, and create a baseline for determining what mandatory capabilities should exist for security technologies that can be used for capturing and detecting malicious activity in control system networks.
The study team used a two-pronged approach to ensure a complete and robust sampling of existing security technology requirements was obtained. The study team had access to proprietary, commercial, open-source, and research systems. Where appropriate, the technology was deployed in a laboratory environment. The study team leveraged specific opportunities to observe traffic analysis capabilities in actual field deployments. By working with clients and partners the study team, was able to assess these capabilities in both a wired and wireless environment. In this tasking activity, Lofty Perch used their capabilities baseline as a foundation for the analysis of several different systems and configurations, and ensured that their approach took into consideration interoperability and interdependencies of both wired and wireless networks.
The study team created specific system scenarios to ensure suitable coverage of plausible architectures. The system architectures types, consisting of both wired and wireless communications, developed for this tasking were:

System Type 1: SCADA system comprised of single vendor solution technology, and a common integrated network facilitating communications between SCADA operations and field activities. The system is not connected to any other peer network. The system is connected directly to the Internet with no security countermeasures in place.
System Type 2: SCADA system comprised of single vendor solution technology and a common integrated network facilitating communications between SCADA operations and field activities. The system is not connected to any other peer network. The system is connected directly to the Internet and is protected by a firewall.
System Type 3: SCADA system comprised of single vendor solution technology, and a common integrated network facilitating communications between SCADA operations and field activities. The system is connected to corporate and is protected by a firewall.
System Type 4: SCADA system comprised of single vendor solution technology, and a common integrated network facilitating communications between SCADA operations and field activities. The system is connected to a peer control network via a firewall. The system is connected to corporate and is protected by a firewall.
System Type 5: SCADA system comprised of single vendor solution technology, and a common integrated network facilitating communications between SCADA operations and field activities. The SCADA system is connected to the Internet via a firewall to facilitate a persistent remote connection from the SCADA vendor to a dedicated server on the control network and is connected to corporate (via firewall).
System Type 6: SCADA system comprised of multiple vendor solution technologies, and a common integrated network facilitating communications between SCADA operations and field activities. The system is not connected to any other peer network. The system is connected directly to the Internet with no security countermeasures in place.
System Type 7: SCADA system comprised of multiple vendor solution technologies, and a common integrated network facilitating communications between SCADA operations and field activities. The system is not connected to any other peer network. The system is connected directly to the Internet and is protected by a firewall.
System Type 8: SCADA system comprised of multiple vendor solution technologies, and a common integrated network facilitating communications between SCADA operations and field activities. The system is connected to corporate and is protected by a firewall.
System Type 9: SCADA system comprised of multiple vendor solution technologies, and a common integrated network facilitating communications between SCADA operations and field activities. The system is connected to a peer control network via a firewall. The system is connected to corporate and is protected by a firewall.
System Type 10: SCADA system comprised of multiple vendor solution technologies, and a common integrated network facilitating communications between SCADA operations and field activities. The SCADA system is connected to the Internet via a firewall to facilitate a persistent remote connection from the SCADA vendor to a dedicated server on the control network and is connected to corporate (via firewall).
The study team collaborated with its technology committee of partners and vendors, and found that the system types provided the best representation of architectures while maintaining a manageable number requiring review. The simplified network base was created by using the Lofty Perch training system, and that allowed for timely and accurate testing of a number of different commercial solutions, resulting in comprehensive and useful observations.
The approach to developing normal and abnormal operating conditions and traffic was done both manually and by leveraging commercial technologies. The study team was exceptionally diligent in ensuring the test cases established accurately modeled real-life scenarios and also took into consideration the observations and concerns of project partners working in the stakeholder community. Having an existing control system available for testing expedited the results and allowed for efficient comparison against other research. The information gleaned from the testing allowed the research team to populate the

results matrix to define base requirements that a traffic inspection or intrusion detection system should have based on system type.

SCADA and control system traffic was generated with two models; normal and abnormal, with abnormal being defined as traffic that exceeded standard alarm and event thresholds and could therefore be deemed possibly malicious. The study team chose this approach so that the observations collected would be tied to anomalous behaviour worthy of investigation as opposed to alarms that may simply trigger a system reset by the operator. In short, the procedure for the testing helped define what specific capabilities traffic analysis and intrusion detection technology should have to provide an enhanced security posture (threat focused) above and beyond simple control system maintenance.

The study team performed a rigorous course of testing that could complement both existing research as well as capabilities of current traffic detection technologies. With the goals of the project correlated to improving the understanding of identifying cyber-threat activities in SCADA systems, the study team created a test suite representative of activities as seen from unorganized low-level threat actors to the most advance adversaries. These activities included (in no particular order):

Using standard commercial and open-source traffic analysis tools to capture datasets, and provide a capability to manually create baseline measurements of the normal system operational envelope

Using standard commercial and open-source traffic analysis tools that can capture datasets and automatically create the baseline measurements of the normal system operational envelope

Using commercial and open-source traffic analysis tools that are embedded in other security devices

Using commercial and open-source traffic analysis tools that have extensive capabilities to either collect from (import) or distribute (export) security logs to centralized security management services

Using standard commercial and open-source security assessment tools in a non-customized (i.e. non-SCADA specific) configuration

Using standard commercial and open source security assessment tools in a fully customized SCADA-specific configuration

Using commercial and open-source network and device stress testing technologies to ascertain failure modes and vulnerabilities

Using standard commercial and open-source security technologies and evaluate the impact on SCADA system security profiles depending on the placement of those security technologies

Detailed analysis of how the placement of traffic analysis solutions impact detection, and how detection capabilities are impacted at the network, host, or application level

Analysis of how detection rates change based on whether or not the communications are expected, as well as authenticated or unauthenticated (trusted or non-trusted).

The study team also benefited greatly from the access it had to the stakeholder and vendor community, and during the course of the tasking the team was able to perform analysis on live production systems

during formal assessment engagements. When analysis was not permitted on live production systems, the study team collaborated with the asset owner to discuss the aspects of the research approach, and collected intelligence about the data capture and analysis practices currently being used by the Canadian critical infrastructure stakeholder community.

To facilitate useful conversations for the collection of data relevant to the study, the study team developed a series of questions for the asset owner and vendor. This approach allowed the study team to better understand existing practices that are working in actual field deployments, as well as contrast and compare perceived gaps as defined by the asset owner and vendor community. The framework for these discussions is defined by the questions provided in appendix C of this document.

The results from the activities in Task 1 Subtask 1.1 are discussed in Section 3 of this Report.

Approach to Subtask 1.2: Identify the capability gaps in efficiently detecting malicious traffic targeting SCADA systems, and survey and evaluate the research literature in relation to work being done to improve this capability.

This tasking element was not called out specifically as a unique item in the project plan. However the study team felt it appropriate to assign this activity its own subtask due to the relevance and importance of its output. The initial subtask (1.1) provided for the creation and population of a technical matrix that, when completed, would easily provide direction on how to interpret current and emerging gaps related to technology for detecting malicious traffic in SCADA systems.

Current literature was analyzed in this task, and in many cases this included the review of proprietary documentation provided by vendors and stakeholders. The results section of this report will provide more information on research reviewed.[3] Current trending indicates that contemporary commercial solutions are quite suitable for detecting malicious traffic in control system environments but the success of that detection is highly dependent on the technological expertise used to configure the technology. Although this observation was expected, the approach to this subtask was to go beyond these expected observations. The study team decided that the approach to evaluate the outputs from the prior subtask (used to populate the requirements matrix) could be used in tandem with analysis of security assessment results and interaction with both the stakeholder and vendor communities.

Results from this approach were useful in determining what gaps exist and what needs to be on the development horizon for solutions designed to capture SCADA traffic and detect malicious activity. The results from these activities are discussed in Section 3 of this Report.

Approach to Subtask: 1.3: Evaluate forensic technologies and techniques that can be leveraged to understand the response of SCADA systems to malicious traffic.

Contemporary forensic investigation technologies and techniques are thought to be useful across almost any standard operating platform. Using available research, combined with input from and consultation with project stakeholders, the study team took the approach that data acquisition and collection of incident artifacts are able to be obtained from target system in either a ‘dead’ or ‘alive’ state. The study team looked to contemporary research to guide them in their approach and observed that based on the availability requirements of many industrial control systems the methodologies used to perform forensic analysis must be done on systems that are fully functional and in many cases cannot be taken off-line. In addition, current trending indicates that there is a notable increase in cyber-attacks taking place in the physical memory of a target system. This trending suggests that many of the artifacts needed to understand the impact of malicious activities on an information system, ones that exist in memory, may not be observed using traditional forensics methodologies designed for off-line systems.

In the interest of time and budget the study team chose to focus attention on the Windows operating system as the core operational platform for the majority of contemporary SCADA and control

[3] Due to the sensitive nature of the materials, the report does not provide insight to specific proprietary documentation provided by stakeholders or vendors.

system solutions. This decision was also driven by the fact that almost all of the study partners and asset owners used Windows environments as their base operating system. Based on these criteria the test bed to be utilized at the Lofty Perch facilities were developed on a Windows platform. It was serendipitous that Lofty Perch was active on cyber-incident investigations during the term of the study, allowing for advanced analysis on actual operational SCADA systems. The live systems under evaluation were also based on the Windows platform. It should be noted, however, the study activities were not exclusive to the Windows operating system, as forensic investigation tools for the reverse disassembly of firmware on embedded UNIX systems, particularly for those in the SCADA radio testing portion of the study, were also used. The study team spent significant effort on embedded Linux as well, particularly in adapting open source forensic utilities to extract proprietary files and encoding information for the purposes of reverse engineering. The analysis of contemporary forensics tools for UNIX systems was investigated and predominately used for evaluation of the technology associated with distribution automation and advanced metering infrastructure (AMI). [4]

In the laboratory environment, the study team used the base architectures developed for the previous task and performed various automated and customized attacks on them. In addition, some customized malware (developed prior to study activities) was released on the test bed systems in a controlled manner, with subsequent investigation performed by analysts who were both knowledgeable and not knowledgeable about the method of attack. This provided significant insight to the viability and usefulness of contemporary forensic investigation techniques on SCADA systems.
The methods used for the creation and deployment of unauthorized and malicious traffic were the same as those used in previous task elements. For the analysis of forensics technologies there was also the inclusion of malware and malicious mobile code. Where possible, the study team made attempts to modify program payloads to have a specific impact on specific processes unique to the control system.

1.2 Findings and observations

Subtask 1.1: Evaluate existing security technologies in view of identifying the best solutions for capturing wired and wireless SCADA traffic and detecting malicious activity.
Figure 3 (page 23) provides a matrix showcasing what requirements would be necessary for effective traffic capture technology that can be used for detecting malicious activity on a SCADA network. This was cross correlated with existing types of technology and sampled SCADA configurations studied.
The study team ensured that their approach took into consideration interoperability and interdependencies of both wired and wireless networks, and leveraged their technical subject matter expertise to create test-bed environments that addressed both. The acquisition, configuration, and deployment of commercial traffic capture technologies, whether wired or wireless, were very straightforward. As cited in the interim study report, network analysis tools are well-suited for analyzing net flows and traffic flows in industrial automation domains, and can include capabilities to analyze field traffic when protocol converters are used. There is a considerable amount of commercial and open source research dedicated to the development of enhancing traffic analysis and anomaly detection capabilities for SCADA, with the majority of the market leading commercial vendors providing for the integration of intrusion detection signatures into their suite. Of particular importance was the recognition of emerging independent research

[4] Although the study activity was inclusive of both wired and wireless environments, the project focus was on traditional SCADA systems. Although AMI is often considered a vital component of energy management operations, by definition it is not usually considered part of a SCADA system and as such analysis of AMI security issues is beyond the scope of this report.

provisioning for the development of pre-processors that could facilitate straightforward analysis of captured traffic using contemporary intrusion detection technology.[5]

The study team worked with asset owners and integrators to evaluate the issues related to the placement of traffic capture technologies and the access to mission-critical network devices in which technologies could be deployed. Unlike contemporary IT infrastructures, access to critical network routing and gateway systems, as well as direct access to the command and control networks for automation operations, is nontrivial. This is due both to local operational requirements and to separate governance for IT and engineering domains. Although the technology explored was passive in nature, the mandatory requirements for system availability and integrity (as opposed to confidentiality) provided the study team with direct exposure to the issues related to deploying security countermeasures within industrial automation domains. Although the impediments were not always technical in nature, the cultural requirements and security aspects associated with how the asset owner protects their networks can create barriers to the deployment of traffic analysis and intrusion detection software in SCADA operations environments.

The observations collected from the research addressing commercial, open-source technology, and emerging research strategies all conclude that the approach used by traffic capture and intrusion detection systems, when used passively, is applicable to control systems environments. However, it was observed that as the complexity of the control system network increases so does the effort required to discern between different traffic flows, the volume of the traffic, and the co-mingling of datasets that can be traversing the same network. When systems range in complexity (analogous to those architectures developed for the study), the accessibility to corporate, peer, and Internet information enclaves can radically impact the work effort associated with developing effective traffic analysis capabilities with the intent to look for malicious traffic. The decision for an asset owner to create a parallel or integrated traffic analysis system for SCADA data requires clear control objectives and mature IT processes which are not developed in all asset owner organizations.

In all cases however, the results suggest that the most effective approach to looking for network traffic that could be malicious in nature is one that involves looking for deviations from expected traffic (as opposed to trying to develop signatures against known and unknown attacks). Contemporary commercial and open-source offerings provide an entire suite of various technologies able to provide this service. The ability to compensate for the uniqueness of control system specific traffic lies in the ability to learn traffic envelopes and create triggers to detect deviations from them. These observations align well with the research reviewed for the study, and there is clear trending in the commercial domain that indicates the work done in the academic and research community is quickly being integrated in contemporary traffic analysis techniques and technologies.

The common thread in the literature reviewed was that the fundamental problem in analyzing network traffic to identify malicious behaviour in SCADA domains is correlating traffic type, volume, and payload analysis to recognize possibly malicious activity. As the study focused on network communications, it was clear that the modernization of traditional serial-based protocols to TCP/IP has reduced the complexity associated with capturing and analyzing these communications. In fact, almost every modern traffic analysis tool makes clear concessions for the control system protocols over TCP/IP, IPv4 and does an excellent job of mapping port, timestamps, and payload. However, these protocols have primarily been encapsulated in TCP/IP. Session management, identity and authorization along with other features of modern application and data protocols have not been implemented.

By referring to the matrix in figure 3 the reader can review what the study emphasized to be the fundamental elements for effective traffic analysis allowing for the ability to detect anomalous behaviour. The analysis is intended to provide quick reference to readers and provide insight on the evaluation of existing security technologies (and their capabilities) for capturing wired and wireless traffic and

[5] The study focused on capturing SCADA traffic and detecting malicious activity. This focus allows for the easy extrapolation out to intrusion detection, but the methodologies surrounding intrusion prevention exceed the scope of this study and are not included in this report. The reader is encouraged to research the concept of intrusion prevention as applied to industrial control systems.

detecting possible malicious activity. The study team determined that the format of this matrix should be structured to allow for readers to cross correlate traffic analysis and malicious behaviour detection methods with their own system architecture type. This approach proves valuable to the stakeholder, as a simplified discussion of what technologies either work or do not work cannot provide the level of granularity required to deliver value to the stakeholder. After the incorporation of requirements derived from interactions with stakeholder community, the vendor community, and the Lofty Perch test bed environment, nine (9) core functional areas that can be applicable across the entire family of study architectures were uncovered.

Create Packet Capture Files

All of the research and interactions with the stakeholder community, as well as those with the vendor, demonstrated that a requirement to be able to create packet capture files or traffic files that can be converted to common packet capture format is mandatory. During the study, it was determined that the most common path for analysis was using the TcpDump capability and the incorporation of the output files into any analysis tool such as Wireshark[6]. The use of these two technologies was pervasive across the entire study and was a component of almost every piece of commercial and research technology evaluated. More importantly, from interviews with the asset owners, it was noted that the personnel from the stakeholder domain responsible for the analysis of traffic within control system environments usually have an excellent understanding of these tools and use them exhaustively in data analysis programs. Any technology to be used for SCADA traffic analysis (with the intent to detect malicious behaviour) or any technology to be incorporated as part of an intrusion detection or intrusion prevention system will use these elements.

Deploy in Either Active or Passive Modes

The study derived 10 plausible SCADA architectures to account for the extensive diversity and uniqueness of industrial automation used in the real world. The factors associated with the integrity and availability requirements of these different systems create a situation where no two control systems have exactly the same restrictions on deploying security controls. This became very clear in the laboratory analysis and was underscored during the discussions with the stakeholder community. It is in consideration of this issue that one of the requirements for traffic capture is an analysis capability that can be deployed in either an active or passive mode.

There has been considerable discussion about deploying traffic analysis capabilities (as a security function) as a real-time , in-line countermeasure in mission-critical industrial automation domains, as there is always a concern that the data packet capture and inspection methods can introduce latency into the communications. Obviously, for many entities, the introduction of any latency into communications is often unacceptable and the deployment of active and in-line traffic analysis technologies is simply not possible. It is also important to mention that many of the commercial security solutions that involve active analysis of traffic flows provide the user with the opportunity to have the system take reactive measures when possibly malicious traffic is detected. This can result in modifications to the data stream in an attempt to get the communications to conform to expected and allowed behaviours.

The study indicated that asset owners, who have varying degrees of availability requirements, desire an ability to deploy traffic analysis in either an active or passive mode. This requirement is in conjunction with the other requirements as illustrated in the matrix. However, the reader is reminded that the results from this study indicate that requirements do change based on system type.

Deploy at a Switch or Firewall

[6] This observation refers to the technology in question using tcpdump as a core element of its package capture, and not simply using tcpdump itself as an isolated diagnostics tool.

The study team found this requirement initially somewhat of a surprise, as some early assumptions were made suggesting the asset owner has complete control over how SCADA traffic analysis was done. In addition, the extensive field experience the study team had in assessing SCADA and control system networks suggested that perimeter firewalls and switches were either deployed and managed by the corporate IT facility or were built, deployed, and managed only by the vendor or integrator. The study was able to ascertain that if the capability existed to deploy traffic analysis within a switch or a perimeter firewall was possible, then it is a viable option that should be considered.

A switch or firewall traffic analysis capability, in the context of this study, would be most useful if able to facilitate the delivery of packet capture files as well as being able to be deployed in either an active or passive mode. The study indicated that those firewalls with packet capture capability do not necessarily require the ability to assess data in the passive mode due to the nature of the firewall core function (i.e. deep packet inspection). The study also showcased the fact that while switches offer a tremendous opportunity to do traffic analysis, it is often the case that the asset owner themselves do not have the permissions or ability to manage the network switch that was configured and deployed by the vendor or integrator.[7]

Send Outputs to SEIM Systems

The study showcased that the complexity of a control system environment greatly dictates the extent to which traffic analysis needs to be performed, and how important it is to ensure there is aggregation of the results of those analysis outputs. Contemporary security countermeasures in the IT domain often deploy aggregation techniques to correlate security event and incident information, and the systems are aptly called Security Event and Incident Management (SEIM) systems. The goal of the systems is to collect disparate security information and present it in a manner to provide security operators and analysts a comprehensive view of the security health of their operational environment.

During the study tasking, it was surprising to learn that the stakeholder community is becoming very aware of these technologies and the value proposition they have for protecting mission-critical control environments. However, the stakeholder community is also quickly realizing that not every commercial offering is a suitable solution for SCADA environments. As the systems have become more complex, and the asset owner is required to deploy traffic analysis and anomaly detection across a broader domain, these correlation capabilities are growing in acceptance. The success of these aggregating systems is entirely dependent on the capability of constituent field devices (those capable of creating security incident information or logs) to 'feed' them with appropriate data. As such, regardless of the security technology used for capturing SCADA traffic (with the intent to detect malicious activity) the traffic capture function must have the ability to feed these aggregators and do so with the expectation the SEIM can interpret the inputs.

The study results suggest that this capability is not always mandatory but rather optional. The study found that the complexity of the SCADA system can dictate whether or not such a capability should be present, and concluded that when an asset owner is requiring ongoing comprehensive analysis of the security health of their control system that this feature may be required.

Learn Normal Operational Envelopes

Although the thrust of the study area was to determine what existing security technologies provide the best solutions for capturing wired and wireless SCADA traffic and detecting malicious activity, a by-product of the research indicated that the expected control system behaviour can be used to accelerate the detection of possibly malicious activity.

In each of the architecture samples, as well as observations from real world environments, and interactions with both vendors and stakeholders, the detection of malicious activity in a control system

[7] One of the more interesting elements that resulted from working with asset owners in the study was that the integrators and vendors often provide unmanaged switches in the control system environment, therefore extensively limiting the asset owner's capability to implement security centric traffic analysis capabilities. The cultural or implementation issues related to this are beyond the scope of this research, but it is provided here as the study team found the observation noteworthy.

environment is directly tied to understanding anomalies from expected data transactions. In SCADA domains, there are regular communication patterns that are generated during normal operations. As the systems are designed and deployed to often perform highly repetitious and highly efficient processes, the architectures are deployed with a fixed and known number of network elements and operate with a limited number of protocols.[8] These aspects, in addition to the collection and management of regular process parameters, facilitates information that can be used to create upper and lower thresholds between which a SCADA system is considered to be 'well behaved' when functioning. If the system communication activities can be captured over periods of time, and under various operational scenarios, it is usually straightforward to create an expected behaviour 'envelope'. From this behaviour envelope operators can create parameters to be used in traffic analysis and intrusion detection systems, and have those systems trigger for possibly malicious activity when the bounds of the expected behaviours are exceeded (either high or low).

Although the study team expected that this requirement would be straightforward in understanding, investigation into the techniques and technologies used for this capability yielded various approaches. Based on this information it became very important to understand these approaches from a technology perspective, as well as understand how those approaches integrate with other fundamental capability requirements for traffic analysis and intrusion detection for SCADA systems.

The evaluation of literature and current commercial offerings indicated that the most useful output from data capture solutions, from a security perspective, is in the form of anomaly and attack detection systems. The research suggested a range of these capabilities exist, from basic configuration of open-source tools to the deployment of algorithm-based pattern matching and anomaly detection engines. Regardless of the technology however, it was very clear that the most efficient use of data capture technologies for detecting malicious behaviour will exploit the fact that the SCADA system operates as 'well behaved' and provides a number of communications attributes that are easily defined.

The study team determined the parameters and technical attributes that would prove most beneficial in a data capture system designed to model and learn the normal operational envelope. In the most basic configuration, capability requirements for such traffic analysis technologies may include (in no particular order):

Source IP and port of data flow between devices

Destination IP and port of data flow between devices

Range of fixed number of network devices and IP addressing schema

Scheduled communications including protocol type and timing (includes consideration for detection of the absence of scheduled communications)

Ingress and egress monitoring for critical trusted devices

Payload analysis

Device-to-device 'legal/allowed' data transactions

Communications to devices specifically deployed as a security countermeasure[9] (i.e. 'canary')

Consideration for alarms and events

Consideration for network diagnostics and enumeration[10]

[8] Depending on the architecture, this number can large. Generally speaking, however, there is usually only a single protocol being used within a particular architecture enclave and in this study was limited to those protocols using TCP/IP (Ver. 4) . Multiple protocols can be used over disparate architectural elements, and it is through protocol conversion that data transcends across domains.

[9] A canary is a pre-established point of presence on the network with no specific function and no permission to communicate with other devices. Any communication to it could be a sign of abnormal behaviour or malicious activity.

[10] The networking tools and technologies used for these activities are identical to those used by adversaries in the early rounds of enumeration and target identification, and thus required special attention. This issue is beyond the scope of the study but continues to be an area of focus for working groups, security technology vendors, and asset owners.

Configurable with Customized Signatures

During the research phase, the study team worked closely with asset owners that have either deployed traffic analysis capabilities or are in the process of deploying them. Those entities that had an advanced understanding of cyber security requirements for control systems clearly indicated that any traffic analysis capability, especially those designed to support intrusion detection solutions required the capability to be customized with signatures specific to the operational environment. Although several commercial solutions evaluated during the study indicated that SCADA and control system signatures are widely available, many of the current solutions offer signatures that are unrelated to a large majority of asset owner architectures. With that, the study was able to conclude that those traffic analysis capabilities capable of being tuned (using very specific and customized detection signatures) show the most promise for detecting malicious activity in SCADA systems.

The study uncovered an exceptionally broad range of traffic analysis technologies available to facilitate for the uniqueness of SCADA operational environments, with the simplest and most cost-effective solutions being those from the open source marketplace. At the other end of the spectrum resides commercial and research technologies that require some monetary investment but also some advanced technical capability to maximize the solution offering. Interactions with asset owners suggest that although no-fee technology is attractive, the most effective solutions appear to be those involving minimal cost expenditure as it pertains to the acquisition of the technology and the cost associated with tasking personnel to oversee the management of the traffic analysis solution.

The testing in the laboratory environment proved that simple modification of common traffic analysis tools can result in an effective capability for the detection of malicious traffic. Yet, there is clearly an opportunity for more advanced anomaly detection capabilities to provide value to the stakeholder community. The study showed that there are three fundamental aspects with regards to how technology can support traffic analysis and the detection of malicious activity in SCADA systems.

The fundamental aspects of technology that has the ability to be customized from a signature perspective include:

Template or primitives language for specifying patterns in data streams

Scripting language for the conditional linking of signatures in rules

Ranking of data elements to represent architecture assets and criticality

The study also demonstrated that an organization that has a good understanding of their cyber-risk (as it relates to assets and consequence) may be more successful in deploying effective traffic analysis and anomaly detection solutions. This observation highlights the importance of having the necessary subject matter expertise to deploy and manage traffic analysis systems in control system environments, and that the proper customization of anomaly detection systems is critical to detecting abnormal and possibly malicious traffic in the most efficient way possible.

The study demonstrated that when these three capabilities are present in the network analysis technology they can be appropriately tuned to perform effective anomaly detection, thus leading to a better understanding of possible malicious behaviour. Currently, as per study activities, it has been determined that almost all contemporary network monitoring and intrusion detection systems available on the market provide the capability to meet the requirements as listed above.

Deploy as Network Based

The study team anticipated that one of the requirements was the ability for technology to be deployed as a network element. However, it was interesting to discover that the range of possible networking environments where the traffic analysis/intrusion detection capability would need to be deployed was quite extensive. These findings emphasize both the requirement for subject matter expertise and engineering knowledge, combined with the fact that event correlation may be a requirement when trying to aggregate information. The list of useful capability requirements (network based) that a SCADA traffic analysis solution should have is extensive, and includes:

The technology must be able to adapt to traffic mirrored passively to network taps.

The technology should be able to replay traffic captures out of band from live systems.

The technology should be able to output full file reads and alarming to centralized aggregators across either a dedicated network or an out of band communication.
The technology should be tuneable to:
Ethernet
Fiber-optic
Serial (USB)
WiFi
900 MHz FHSS
Reserved radio band technologies

Deploy as Host Based

As the study targeted the evaluation of existing technologies for both wired and wireless SCADA environments, the study team assessed how important the placement of the technologies in the operational domain was. As the maturity of traffic analysis and intrusion detection systems is accelerating to accommodate the needs of diversified asset owners, including those in the control system domain, traffic analysis is usually done as part of a defense in depth strategy. With that, the concept of deploying traffic analysis capabilities at the host level was also reviewed in the study. This review was done by using open-source literature, collecting information from stakeholders and asset owners, as well as investigation of host-based analysis in the project test environment.

The deployment of a host-based traffic analysis capability enhances the ability to create a comprehensive intrusion detection system, but not all system types would find this beneficial. The ability for a traffic analysis function to be deployed within a host environment appears too only enhance the security value of the simplest systems. In addition, even on those simple systems, moving the traffic analysis capability increases the risk of introducing a degradation of performance in the host environment. Thus, as was reflected in the testing environment, there is concern about whether or not traffic analysis and intrusion detection should actually be deployed in host domains. The testing indicated an increase in performance requirements for the hosts running traffic analysis, and unless the supporting hardware and operating system is provisioned with sufficient memory traffic analysis should remain in the network enclave. However, the study suggests (as verified by stakeholder interaction) that as the system complexity increases so does the requirement for broader, qualitative network intelligence. Security technologies that have the capability to monitor net flow and connection states at the host level can provide a second-level of data useful in the detection of malicious activity. In some instances, the study found that the security health of complex SCADA architectures can be better understood by collecting information from the host elements in addition to traffic volume and types collected at the network level. The study showed that in addition to network analysis, host monitoring could provide information regarding the detection of malicious activities that are generally not seen at the network level. This could include system file modification attacks that manifest on the host itself or provide insight to attacks that can't be detected over encrypted channels.

Aggregated information involving network statistics and connections, particularly those that exhibit connections outside of normal operational envelopes (and connections that may be from unauthorized devices), can help detect malicious traffic targeting specific SCADA system elements. Analysis of this topic in collaboration with stakeholders and asset owners indicate that this solution, although interesting to them, is suitable for more complex and in turn less pervasive and numerous, control system architectures. Study partners indicated that this solution could prove useful but would require a significant amount of subject matter expertise in the development, configuration, deployment, and management of the capability.

Ensure a Small Operational Footprint

The requirement for the traffic analysis solution to have little or no impact on the efficiency and operations of the SCADA domain cannot be overstated. During the study, there was not a single instance of any stakeholder or asset owner suggesting that the deployment of traffic analysis and anomaly detection capabilities did not need to take system performance into consideration. Using the various architectures developed for the test environment the study team was able to ascertain that a large operational footprint of the traffic analysis capability, as well as those involved in anomaly /intrusion attention, can in many cases impact operations. Although passive monitoring does not necessarily imply a noticeable impact on processing resources from network switching equipment, the process of aggregating the analysis information and sending it over critical networks can impact system availability. In typical production networks, passive collection is achieved using separate or overlaid networks that do not use the same transport and processing resources as production data.

The emerging requirement for the traffic analysis capability (that is to be used in support of intrusion or anomaly detection in SCADA environments) suggest deployment options be available to allow the operator to get the analysis data locally or through the communications channel of their choice. The study did show that most traffic analysis capabilities designed to support the detection of malicious activity support this requirement, and these capabilities are implemented specifically to meet the aforementioned concerns.

FUNDAMENTAL CAPABILITY REQUIREMENTS FOR TRAFFIC ANALYSIS AND INTRUSION DETECTION FOR SCADA										
	Ability to create packet capture files (.pcap)	Ability to be deployed in either active or passive modes	Ability to be deployed at a switch or firewall	Ability to send outputs to SEIM (aggregator)	Ability to learn normal operational envelope (modeling)	Ability to be configured with customized signatures	Network Based	Host Based	Maintains small and no-impact footprint	Comment
SCADA System Type 1	YES	YES	OPT	OPT	YES	YES	YES	OPT	YES	Host based could also be deployed on the SCADA system elements
SCADA System Type 2	YES	YES	YES	YES	YES	YES	YES	OPT	YES	
SCADA System Type 3	YES	YES	YES	OPT	YES	YES	YES	OPT	YES	
SCADA System Type 4	YES	YES	YES	YES	YES	YES	YES	OPT	YES	Aggregating data to and from peer networks is critical to understand envelope
SCADA System Type 5	YES	YES	YES	YES	YES	YES	YES	OPT	YES	
SCADA System Type 6	YES	YES	OPT	OPT	YES	YES	YES	OPT	YES	
SCADA System Type 7	YES	YES	YES	OPT	YES	YES	YES	OPT	YES	
SCADA System Type 8	YES	YES	YES	OPT	YES	YES	YES	OPT	YES	
SCADA System Type 9	YES	YES	YES	YES	YES	YES	YES	OPT	YES	
SCADA System Type 10	YES	YES	YES	YES	YES	YES	YES	OPT	YES	

Figure 3: Requirements for Traffic Analysis Capabilities to Detect Malicious Behavior in SCADA Systems

Subtask 1.2: Identify the capability gaps in efficiently detecting malicious traffic targeting SCADA systems, and survey and evaluate the research literature in relation to work being done to improve this capability.

With the focus of the tasking looking to identify capability gaps in technology that can be used to detect malicious traffic targeting SCADA systems, the study team looked at the current baseline requirements for traffic analysis technologies as defined by research and stakeholder requirements. This data was then analyzed and cross correlated with some of the more salient conclusions derived from actual control system cyber-security assessments and the trending in academic and commercial research.

Analysis showed that the existing security technologies developed for traffic analysis and detection of malicious activities in networked environments can be tuned and customized to accommodate for the uniqueness of SCADA and control system environments. The requirements of those technologies, depending on the type and complexity of the integrated SCADA architecture, are defined in the matrix associated with subtask 1.1 of the project. From those observations it becomes clear that the usefulness and effectiveness of these technologies is dependent on the subject matter expertise of the personnel deploying the solution, as well as the technological ability for the system to understand (or learn) behavior patterns associated with the control system.

These observations suggest two notable gaps associated with contemporary technology that can be used to detect malicious activity towards SCADA systems. As some gap associated with the technical capability to configure and manage the systems is related to human expertise, commentary on user education pertaining to the configuration of security technologies is beyond the scope of this research. However, such discussion is addressed later on in study deliverables.

The gap associated with how current analysis technology and its ability to create or auto-tune anomaly detection engines is being reduced. However, this comment is limited to the discussion of SCADA and industrial control systems as recent advancements in this area are based in leveraging the information regarding static operational environments and well behaved systems. Analysis of the requirements matrix, specifically developed for the capabilities that should be fundamental for traffic analysis and intrusion detection systems for SCADA, facilitates for the discussion of emerging requirements necessary to meet the rapidly changing landscape of cyber threats to SCADA and industrial control systems.

A fundamental gap that is ubiquitous across much of the current commercial technology landscape is the ability for the traffic analysis or intrusion detection system to define an operational envelope that is sensitive to zero day attacks. Although much of the commercial landscape offers mechanisms to detect against unknown attacks, perhaps those with no viable intrusion signature, contemporary behavior analysis solutions are not uniquely designed for process control environments. The absence of solutions that are specifically designed to accommodate for the uniqueness and nuances of SCADA architectures showcases a gap between current solutions and those needed to mitigate emerging threats.[11]

The obvious requirement for subject matter expertise and human intervention for the management of the systems is a significant problem. The rate at which subject matter expertise can be optimized to meet the growing cyber-threats against SCADA systems is slower than what is required. This presents a rapidly emerging requirement for anomaly detection to be able to visualize ongoing attack activities, prioritize attack elements, and assigned criticality to possibly malicious traffic. More importantly, as the complexity of the control system increases, these capabilities need to transcend network boundaries and analyzing intelligence collected across disparate cyber-assets. The gap that is deduced from this is that solutions need to be able to provide knowledge about specific attacks without actually knowing about what kind of attack is happening. Technology that provides model- based anomaly detection, leveraging a verified and well-known behavior model of the SCADA system, could facilitate for better visualization of system health and timely human interaction. This human interaction could result in either optimization of the industrial process in question or the refinement of security countermeasures necessary to protect the control system communications infrastructure.

[11] The emerging threat landscape indicates that next generation attacks will incorporate a variety of different methodologies traditionally used as separate attack components. The concept of zero day vulnerabilities is not new, but how a system is able to manage unknown vulnerabilities in the absence of intrusion detection engines is problematic. Defending against comprehensive cyber-attacks that incorporate traditional and unknown attack methods requires a definitive understanding about the behavior the system as well as appropriate triggers used to signal deviation from expected behavior.

Anomaly detection in process control systems is not new, but anomaly detection for security purposes is an emerging domain of interest. In developing traffic analysis solutions for capturing data that could be indicative of malicious activity, it becomes imperative that incidents and alarms generated from deviations of the normal operational envelope be understood as malicious and not just normal system nuances. One of the reoccurring problems as observed in the study, as well as cited by stakeholders and study partners, is that current detection technologies, when deployed on SCADA systems, often alert on activity that is unusual but is not malicious. With that, anomaly detection systems that have learned the SCADA system environment can often fail in detecting malicious activity when the malicious activity is persistent and erroneously interpreted as within the normal operational envelope. This observation suggests that in addition to the development of technology to meet the emerging needs of control system asset owners, specific instruction on how to deploy the technology in a manner that mitigates these issues is also required. The study team felt it important to cite these issues in addition to those related specifically to technological requirements.

Subtask 1.3: Evaluate forensic technologies and techniques that can be leveraged to understand the response of SCADA systems to malicious traffic.

One of the more interesting aspects of the study correlates to the requirement to understand available forensic technology and techniques that can be used to investigate incidents on industrial control systems. The verbiage used in the description of the subtask is somewhat awkward, but the study team interpreted it to mean that the focus should be on the evaluation of forensic technologies that can be used on SCADA systems in the event malicious traffic has actually resulted in undesirable behavior.

The amount of available research related to this topic is exceptionally limited, with only a few publicly available documents concentrating directly on the subject. In the context of this project, the study team leveraged their field experience working on actual cyber-investigations on control system environments and performed investigations in the test bed environment. The fact that the study team has been directly involved in the development of recommended practices and procedures pertaining to investigative methods on SCADA systems, the experience showed that testing and analysis should focus on modern computing environments. Past experience, combined with the research done through the US Department of Homeland Security and the US Department of Energy suggests that contemporary forensics analysis on legacy systems with limited networking capability and immature memory functions is challenging. This is not to suggest that forensics activities are not possible on these systems, but the broad requirements of personnel, experience, and access to vendor engineering to investigate anomalies in legacy control systems (anomalies that could indicate malicious activity) creates a problem that is very difficult to solve. Current strategies and research suggests that the best way forward is to focus on modern SCADA systems and align investigative techniques with current and future system types.

As has been proven in real-world deployments and duplicated many times in the laboratory environments, including work done during the study tasking, contemporary forensic investigation technologies are suitable to perform cyber-investigations on SCADA systems. However, the results from the study reiterate the complexity associated with not ‘what’ technologies are used but rather ‘how’ they are used. Traditional forensic technologies and techniques have been designed and deployed to operate on information systems that are available to be taken off-line, imaged, backed up, and analyzed at the discretion of the investigator. The study emphasized that the opportunities for investigations to be performed on SCADA systems that have been completely removed from the operational environment are rare. The primary reason for this is that the information resources used in SCADA and control system environments have availability requirements that often greatly exceed those demanded by traditional IT infrastructures. Many industrial automation systems responsible for critical infrastructure activities, such as energy production and

management, water, transportation, and natural resources require that the system operates in a perpetual high availability mode and only under duress or extreme conditions can be taken off-line.

When an information resource critical to the operation of a SCADA system has been impacted by malicious activity, unless there is an impact to the safety and reliability of the system the resource is most likely going to remain operational. This can impede the ability for an investigator to get access to any inherent artifacts that provide insight to the nature of the malicious activity and the impact it has on the system. As such, investigative methods that facilitate for the capturing of real-time memory artifacts play a significant role in understanding the response of SCADA systems to malicious traffic and attacks. The architecture in which the impacted information resource resides is also important, as architectures that provide for redundant operations can facilitate for short-term direct access to impacted assets so backups and image capture can be performed.

During the course of the research the study team had the opportunity to perform real-world forensic investigations on SCADA systems and compare the findings to results from their laboratory-based testing. Not surprisingly, the results found that when impacted systems are off-line and available for direct interaction, the current commercial landscape of forensic investigation toolkits provides a wide variety of applicable and useful techniques and technologies. Generally speaking, standard investigation techniques regardless of the technology selected yields the same results. The choice of technology is at the discretion of the investigator, and the usefulness of the analysis performed is defined by the experience and qualifications of the investigator.[12]

Regarding live targets, for systems that were impacted by malicious activity and could not be removed from the operational environment for analysis, the observations yielded new insights pertaining to how forensic investigations can be done on mission-critical SCADA systems. During the investigations performed, as well as during the lab-based testing, the most obvious requirement for performing real-time forensics on a control system is that the footprint of the memory capture mechanism is a small as possible. This requirement, in addition to capabilities facilitating for the investigator to look at certain processes in action, is vital in several ways. Firstly, as the system under investigation is currently operational there can be no risk to impact the performance and safety of the system by the introduction of an alien process. Secondly, the investigative method has to provide minimal influence of the artifacts collected in the event analysis is intended to support legal activities (i.e. prosecution).

The study found that under most cases tools that are designed to capture entire active memory snapshots (as a point in time) worked well. The scenarios where the unauthorized and malicious activity was introduced intentionally to the system and the investigating team had predetermined knowledge, investigating technology and techniques yielded expected results. In the study activities that involved real world investigations, and the source and extent of the malware actions were unknown, secondary and tertiary investigation activities were required following the capture of live memory. As speed of the investigation is a concern, the mechanism for interfacing with a live system for memory capture was also studied. It was demonstrated that those tools with the capability to interface via removable media were deemed most useful, but when the malicious activity involved malware that used portable media as a transport mechanism, the procedure for managing the collected artifacts on a now-infected archive had to be considered.

The analysis activities in the study demonstrated that those forensic capabilities capable of storing files in multiple formats is useful, and compression system that can accommodate for low storage capture devices compensates for control system devices using large RAM. This capability proved exceptionally useful when the investigative technology empowered the analyst to collect information on specific processes that were running and, if required, push all available executable code into RAM for analysis. This is exceptionally important for the investigator when

[12] Success is also determined by the investigators understanding of the SCADA system under analysis.

there is a thorough understanding of SCADA system executables and libraries, and can greatly enhance and investigators understanding of what (if any) SCADA-specific processes that have been impacted. Even though the detailed information about process structure and behavior is usually only known by the vendor, the collection of the information for later analysis can prove invaluable when direct access to impacted processes can be analyzed. The capability that can allow an investigator to specifically target certain processes looking for malicious or nefarious activity, although very useful, should only be done after an initial RAM capture has been performed.

Forensic technologies and techniques useful in real-time SCADA environments should also include the number of specific system diagnostics tools and configuration capture mechanisms. Common standard investigation procedures take into consideration the role the device under investigation plays within the network architecture. Generally speaking, elements in control system and SCADA architectures tend to have well-defined and specific relationships with other information resources in the operational enclave. Having access to configuration information that defines routing, static connections, source and destination port, and connectivity state provide significant information to complement the data captured during live memory analysis. The cross correlation of artifacts from live memory analysis with system information and can yield significant intelligence about an incident.

Working in a Windows environment, the study team found that there were a number of SysInternal operations that are beneficial when investigating operational control system devices. Depending on the requirements of the investigation, and assuming an initial primary memory snapshot has been performed, SysInternal command functions can be used to harvest information to compare against known operational attributes of the SCADA system. The study team found this approach useful, as the uniqueness of the control system and the understanding of its expected performance provides a foundation for a very significant analysis capability. SysInternal commands provide for a number of data acquisition capabilities that can be utilized during an investigation on a live system. The study team reviewed a broad range of acquisition commands, and determined that the most useful (from a control system perspective)[13] include:

arp. exe

This command, using the '-a' argument to list all existing entries for address resolution, provides the investigator specific information to cross correlate against known and expected address entries in the device. Understanding that control system environments are often developed with strategic intra-communication architectures between critical devices, the information collected from this command can be used to compare against expected address listings cited in architecture diagrams and existing connection states. The study showed that the information collected from this command provided specific and detailed insight to the modifications that would most likely be made to a SCADA networking component if compromised by malware or an adversary.

ipconfig. exe

Using the '/all' operator, the investigator will get a complete list of network configurations within the target device being assessed. With an understanding of the expected network configuration of the device, combined with knowledge of the device placement in the architecture and expected communication pathways, information collected from this command can assist in the identification of compromised systems. Taking into consideration the impacts and consequences of successful adversary attacks, including malware, ipconfig. exe can provide information on modifications to configurations that create rogue access channels and covert communication pathways. The study showed that the information

[13] During the course of the study period, the study team was able to experiment on the usefulness of using SysInternal in SCADA forensic operations in both laboratory and real-world environments.

collected from this command, when compared against expected configurations, provided specific and detailed insight to the modifications that would most likely be made to a SCADA device if compromised by malware or an adversary.

netstat.exe

The netstat.exe command allows the investigator to understand the current status related to network connections, protocols, and active IP sessions. Obviously, this information is vital to understanding device operations and provides insight into whether or not the device is behaving as expected. Used in tandem with a detailed understanding of the SCADA network architecture and communications infrastructure, the netstat.exe command will yield information that can be immediately cross correlated with the information captured in SCADA live memory analysis. The study showed that the information collected from this command provided specific and detailed insight to the network modifications that would most likely be made to a SCADA component if compromised by malware or an adversary. In this assessment, the existence of unexpected communications and port assignments provided insight relevant to the intended lateral spread of hostile malware throughout the SCADA system.

nbstat.exe

The nbstat.exe command from the SysInternals library allows investigator to collect information specific to the destination IP sessions currently active. Using the '-S' option, investigator can derive connection state data that can be cross correlated from the intelligence collected from other analysis activities. The comparison of the active IP sessions that a SCADA device has is vital to understanding current behavior, and when information regarding control system processes is derived from the live memory capture, the investigator is positioned to ascertain what, if any, malicious activity or traffic impacted the security health of the SCADA system.

net.exe

The net.exe command was found exceptionally useful to support analysis of existing network sessions within the system under investigation. The outputs using the 'session' argument provided output to be used in comparative analysis information collected using the netstat.exe function. The study also determined that the understanding of the SCADA routing information inside the device under investigation can also provide insight pertaining to the impact of malicious traffic or malware. In these cases, the 'route.exe' command is used and is recommended to be considered a primary component of live control system forensic investigative activities.

plist.exe

In reference to SCADA systems, the study showed that the investigative process is enhanced when there is a solid understanding of active mission-critical processes. Much of the uniqueness associated with control system environments is defined by the processes that are used to perform automation functions. The applications specific to the processed are well defined in the process table, and harvesting active process tables from a system that has been impacted by malicious traffic or malware can provide significant intelligence to the investigator. The study team found that this particular command was perhaps the most useful, as the impacted SCADA process table clearly showed activities that were normally not present in a well behaved system. A review of the particular processes associated with the control system was performed in collaboration with the vendor of the system under investigation, and anomalies created by the malicious traffic or malware were able to be isolated. Using the plist.exe command with the '-t' option provides an output showing the process list tree, and it was found exceptionally useful to compare this output against netstat and net commands.

driverquery.exe

When the investigator has been able to collect intelligence about the normal and expected processes and functions specific to the control system, collecting existing information about active drivers is very useful. As a support query to determining active processes, information about current drivers in a compromised or impacted SCADA system can provide significant insight to how the system has responded to malicious or unwanted actions. The study team found, however, that capturing a list of all installed drivers currently active in a complex control system, when the system is using the Windows environment as a base operating system, creates an analysis activity that is a fairly arduous task. Although the level of effort can be considerable, the results generated to determine the impact of malicious traffic or malware are very useful.

autorunsc.exe

This command was found to be exceptionally useful when being utilized on a system that was confirmed to be infected or impacted by malicious activity. Although investigations tend not to list this command as one to be used in mandatory intelligence collection, SCADA systems and their dependence on 'autostart' applications makes this command perfect for control system investigations. Industrial automation environments, historically, have a significant number of applications that automatically start to support timely resolution of system control. This feature makes these applications an ideal target for malicious traffic and malware, as these system-specific applications will run in a SCADA device with authoritative privileges.

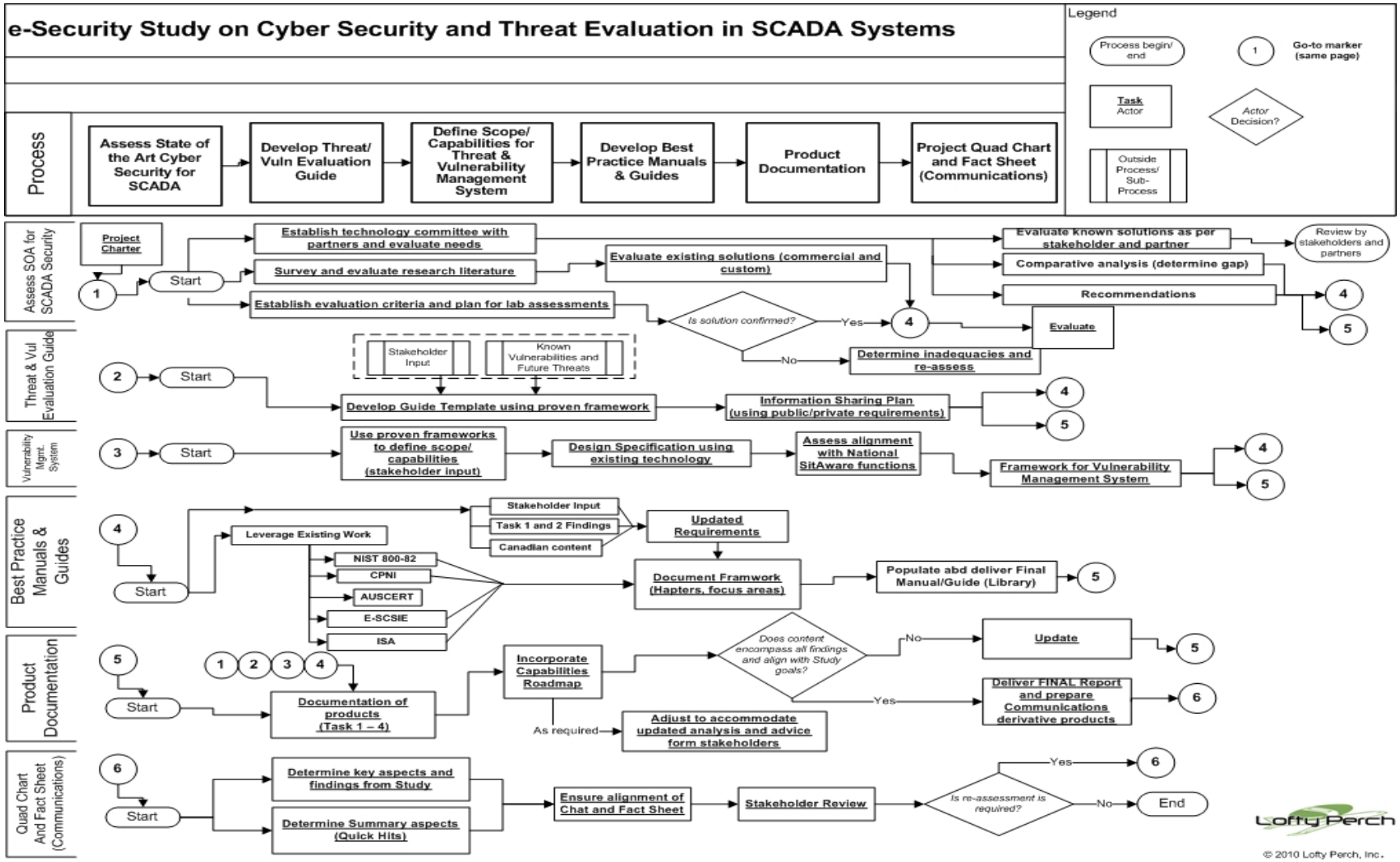
The autorunsc.exe command allows the investigator to collect and analyze information about expected normal behavior start up applications and deviations from expected norms. The output from this command supported the outputs from other investigative tools (SysInternals) used to ascertain existing network sessions and processes. The study showed that the information collected from this command, when compared against expected configurations, provided specific and detailed insight to the modifications that would most likely be made to a SCADA device if compromised by malware or an adversary.

systeminfo.exe

Prior to performing invasive investigative queries, and well after an initial live memory capture has been performed, the investigator should be aware of the operating system under analysis, the service packs associated with that operating system, and any associated adapter information. Information collected from this command should be compared against known and expected values stored by network operators, and deviations from expected configurations should influence the investigation strategy. Specifically, investigators are advised to look at the output to determine system service pack levels and determine what, if any, inherent security countermeasures have been disabled either by the vendor or as the result of malicious traffic.

The study showed that the information collected from this command, when compared against expected configurations, provided specific and detailed insight to the modifications that would most likely be made to a SCADA device if compromised by malware or an adversary. In particular, it was noted that since modifications to service pack levels can have a notable increase in a system's susceptibility to compromise (especially SCADA), outputs from this command can direct how the investigator will utilize SysInternal analysis going forward.

Annex A Project workflow TASK 1



Annex B Selected Research Sources for Task 1.1

1. *"Network Traffic Analysis and SCADA Security"* Mahmood, Leckie, Hu, Tari, http://goanna.cs.rmit.edu.au/~jiankun/Sample_Publication/Network_Traf.pdf
2. *"Communication Pattern Anomaly Detection in Process Control Systems"* Valdes, Cheung http://www.csl.sri.com/papers/HST09ValdesCheung/commPatternPCS-Valdes-Cheung-HST09.pdf
3. "*Detection, Correlation, and Visualization of Attacks Against Critical Infrastructure Systems"* Briesemeister, Cheung, Lindqvist, Valdes http://www.csl.sri.com/papers/PST2010/pst2010.pdf
4. *"Intrusion Monitoring in Process Control Systems"* Valdes, Cheung http://www.csl.sri.com/papers/intrusionMonitoringHICSS09/Valdes-Cheung-PCSmonitoring-HICSS09.pdf
5. *"SCADA Systems Security"*Arjun Venkatraman, http://www.infosecwriters.com/text_resources/pdf/SCADA.pdf
6. *'Tofino'* Tofino," http://www.tofinosecurity.com/products/Tofino-Firewall-LSM
7. "*Industrial Defender"www.indistrialdefender.com*
8. "*Common Cybersecurity Vulnerabilities in ICS_2010.pdf"* http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
9. "*Secure Your SCADA and Industrial Control Systems"* http://www.us-cert.gov/control_systems/pdf/TSWG_Securing_SCADA_V1_Short.pdf
10. http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf
11. "*Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*" http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf
12. "*NIST Guide to Industrial Control Systems Security" http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*
13. "Intrusion Detection in SCADA Networks" Barbosa and Pras, http://www.infosecwriters.com/text_resources/pdf/SCADA.pdf
14. "*Intrusion Detection and Security Monitoring of SCADA Networks"* http://www.isa.org/Content/Microsites988/SP99,_Manufacturing_and_Control_Systems_Security1/Home964/SP99_Presentations/ISA-Users-Spk2-Intrustion-Detect-Security-Monitoring-SCADA-Networks-DPeterson.pdf
15. "*SCADA Forensics with Snort IDS"* Valli, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1528&context=ecuworks&sei-redir=1#search=%22scada%20snort%22
16. "*Enhancing Intrusion Detection in Wireless Networking Using Radio Frequency Fingerprinting"* Hall, Kranakis http://people.scs.carleton.ca/~kranakis/Papers/IDSRFFv4-4.pdf
17. "*The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*, Axelsson http://www.raid-symposium.org/raid99/PAPERS/Axelsson.pdf
18. *" SCADA Security and Terrorism: We're Not Crying Wolf"*RD &D ISS X-Force, http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf
19. "*Using model-based intrusion detection for SCADA networks* " S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes In SCADA Security Scientific Symposium, Miami Beach, Florida, Jan. 2007
20. "Anomaly-Based Intrusion Detection for SCADA Systems" Yang, Usynin, Hines http://entrac.iaea.org/I-and-C/TM_IDAHO_2006/CD/IAEA%20Day%202/Hines%20paper.pdf
21. "*Creating Cyber Forensics Plans for Control Systems"* Fabro, Corenelius http://www.inl.gov/technicalpublications/Documents/4113665.pdf
22. "Using Digital Forensics to Maintain the Integrity of our Nations Critical Infrastructure" http://acm.mst.edu/~security/articles/CCDSandia/SCADA_Forn_2005_Symp.pdf
23. "*Snort IDS for SCADA Systems"* Weaver, https://dl.snort.org/assets/114/Snort_RH5_SCADA.pdf
24. "*Identifying Supervisory Control and Data Acquisition (SCADA) Systems on a Network Via Remote Reconnaissance*" Wiber, Master's Thesis, NPS, http://www.cisr.us/downloads/theses/06thesis_wiberg.pdf
25. "*Security for Critical Infrastructure SCADA Systems"* Hildick-Smith/SANS, http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644
26. *"21 Steps to Improve Cyber Security of SCADA Networks", http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf*
27. *" Recovering and Examining Pewter Forensic Evidence"* Noblett, Pollitt, Presley, http://bartholomewmorgan.com/resources/RecoveringComputerEvidence.doc
28. "*Digital Data Acquisition Tool Test Assertions and Test Plan" DRAFT, NIST http://www.cftt.nist.gov/DA-ATP-pc-01.pdf*

Annex C Interview questions for asset owners

In the interview process, there was an initial question that was asked, from which to branch is a question sets followed: *"Do you deploy and manage any traffic analysis capabilities to look for malicious or abnormal behaviour?"* From this activity, the respondent system architecture was correlated with the template architectures developed for this task.

If 'Yes':

1. Is the technology you use provided by the vendor as an OEM offering or is it an aftermarket commercial product integrated into their solution?
2. Does the traffic analysis solution provide a capability for packet captures for off-line analysis?
3. Is the analysis solution provided passively or is it active and in-line with communications?
4. Is the analysis solution a standalone function or is it embedded in another piece of network technology?
5. Is the traffic analysis solution part of a larger security event and incident management capability you use in your control systems?
6. Does the traffic analysis solution have an intrusion detection capability? If so, does it have the capability to be programmed with customized detection scripts unique to the control system? Can the system monitor and create its own detection engine by learning the system? Both?
7. Where have you deployed your traffic analysis capability? (host, network, application)
8. Is there any noticeable footprint or impact on control system resiliency or availability due to the inclusion of your traffic analysis or intrusion detection activities?
9. Do feel that there are any gaps in contemporary commercial offerings related to traffic analysis solutions for the detection of malicious activity in control system environments?

If 'No':

1. Is there a reason why there is no traffic analysis activity on your control system network? If yes, what are the reasons?
2. Is there any sort of traffic analysis function being provided by any other networking or security devices in the network (as opposed to a standalone traffic analysis and anomaly detection capability)?
3. Do feel that there are any gaps in contemporary commercial offerings related to traffic analysis solutions for the detection of malicious activity in control system environments?

2 Introduction – Task 2- Development of a Cyber Threat and Vulnerability Evaluation Guide

This document provides a comprehensive report on specific tasking as it pertains to Project Task 2 – Development of a Cyber Threat and Vulnerability Evaluation Guide. The tasking in this project area was comprised of three core activities, all of which were performed with the study's primary and supporting objectives in mind:
Define a cyber-threat matrix in consultation with critical infrastructure owners or operators, law enforcement, and the intelligence community.

Perform a review of the known vulnerabilities of SCADA systems, and project future threats and vulnerabilities to provide direction to future research areas.

Identify various approaches to address the privacy concerns of private sector owners or operators in view of sharing cyber-threat and vulnerability reports with the Community of Practice (CoP) and the federal government.

Lofty Perch, Inc. (LPI) and the study team performed extensive research during this study activity, and in addition to collaborating with industry stakeholders participated in numerous seminars and symposia dedicated to understanding the cyber threat landscape as it pertains to SCADA. Understanding that the tasking would result in material to provide for a cyber-threat and vulnerability evaluation guide, activities were performed concurrently to ensure that the materials accounted for vulnerabilities in control systems as well as take into consideration threats from the perspective of the stakeholder community. The report showed that the perceived categories of cyber threat, from the stakeholder community, may have significant impact on critical infrastructure protection and resiliency.

The report showed that the perspectives on cyber-threat to SCADA systems differ between the stakeholder, law enforcement, and intelligence (i.e. national security) communities. As such, the components of the report attempts to close this knowledge gap and takes into consideration that public sector entities have a significant reliance on information from the private sector community. This theme was consistent across all communities of interest engaged for the project, and illustrates how the law enforcement and intelligence communities may be at a disadvantage in terms of collecting information for protecting national critical infrastructure assets from cyber-threats. The study also revealed that asset owners are not convinced that the level of technical capability maintained by the law enforcement or intelligence community is appropriate to fully understand cyber-threat and consequence to critical infrastructure operations, and this may result in a lack of reporting to authorities.

The study indicated that some progress has been made in the establishment of various approaches to address the privacy concerns of private sector asset owners with regards to sharing cyber-threat information, but the existing frameworks may require enhancement. The report showed that not all contemporary solutions for information sharing involve the federal government, but rather it is the growing presence of independent research

and academic institutions that are providing portals for asset owners to share vulnerability and incident reporting. Impediments to information sharing are slowly being recognized, but new approaches are required to create public/private collaboration mechanisms. The study was able to demonstrate that effective mechanisms for trusted collaboration are emerging, and as these agreements mature they may mitigate many of the concerns shared across the private sector asset owner community. The report demonstrated that a significant portion of the stakeholder community remains unwilling to share cyber-threat and vulnerability data with the public sector, even though useful Memorandums of Understanding (MoU's) have potential in helping facilitate intelligence sharing.

It was anticipated that the activities in this study task would present difficulties insofar as obtaining detailed threat information from the federal law enforcement and intelligence communities. This concern was realized, possibly due to the absence of technical expertise within many of the stakeholder environments. However, the study team was able to leverage its extensive network of relationships to mitigate this problem and extract detailed information from the asset owner community (and thus obtain insight from those entities dealing with cyber-threat on a day-to-day basis). Access to various Canadian law enforcement and intelligence entities was limited during the course of the tasking, and as such the study team executed tasking activities in collaboration with law enforcement and intelligence entities with other representatives from the intelligence community.[14]

The results collected from interactions with the stakeholder community regarding perceived threats were surprising, as some domains of interest have not traditionally been considered within the scope of control system/industrial automation. Perhaps the most interesting result was that the study suggests that the asset owner community appears to be predominately concerned with consequences and overall impact of a cyber-event. This is contradictory to the theory that they are primarily concerned about specific threats. The study suggests that the asset owner community is very concerned about the kinetic impact a cyber-incident can have on industrial automation and is less concerned with the threat or adversary (beyond the risk associated with the ever present insider). The stakeholder community feels that a solid understanding of technical vulnerabilities, combined with detailed knowledge about impact when those vulnerabilities are exploited, provides a much clearer approach to proactive and reactive cyber-security strategies. This finding made the development of the evaluation guide elements interesting, as the characteristics associated with threat, and the level of effort to understand them, were very different between private sector asset owners and public sector law enforcement/intelligence agencies.

The study team selected to use a customized version of the CSEC/RCMP Threat Risk Assessment methodology as a foundational framework for the development of the guide. By using this approach, the deliverable would be aligned with the expectations of both the private and public sector communities of interest. This strategic decision may help facilitate for the development of the initial scope and capabilities of a cyber-threat and vulnerability management system for SCADA systems (Task 3), specifically with the possibility of feeding into a national cyber situational awareness capability.

[14] The reasons for this lack of accessibility were many, but the primary reasons included holiday timing, scheduling conflicts, or the fact the federal agency had no designated resource addressing the SCADA cyber-security domain. The study team was able to have limited discussions with some elements within the Canadian government and was successful in discussions with the RCMP Technical Crimes Unit.

The report provided an opportunity to perform an exhaustive review of the known vulnerabilities specific to industrial control systems. To add more value to the report, the study team also reviewed categories of vulnerabilities that are not control system specific but could ultimately impact control system security. It was from this analysis the study team was able to extract a set of plausible future vulnerabilities that could directly impact SCADA security and derive some characteristics of the future threats exploiting those vulnerabilities. Taking into consideration other project tasking, the study team was able to define several strategic areas that could be used to focus future research.

The information collected during this study task showcased that the concerns regarding cyber-threat to SCADA systems are common across the stakeholder community, with deviations in those concerns being attributable to the nuances associated with sector specific architectures. Fortunately, the scope of this task activity was limited to cyber threats and vulnerabilities, thus allowing for the findings to be interpreted by the reader and applied to their architecture as required. The amount of information collected from open source materials was extensive, and when cross correlated with the input from the stakeholder community the study team was able to craft a solid framework to empower any asset owners in creating a customized threat and vulnerability guide.

This document is intended to provide content to be utilized in the comprehensive material delivered in the Final Project Study Report. The material in this document will, where possible, reference other study activities so that the reader will be able to interpret and leverage the information efficiently.

Section 2 is dedicated to discussing tasking and sub tasking activities, with in-depth discussion about the process, procedures, and investigative models used during the tasking. Section 3 discusses the findings and observations from the study activities, and an introduction to the elements used to populate the cyber threat and vulnerability evaluation guide. Section 4 discusses conclusions, followed by Conclusions in Section 5. The appendices provide project workflow, as well as an introduction to a conceptual framework that can be used to enhance information sharing using the attached memorandum of understanding.

Lofty Perch recognizes the extensive support it received from its in-kind partners during the tasking activities, and in the final report deliverable will (wherever possible) be citing them by name. During the development of this and other report content it was deemed necessary to withhold the identity of partners due to the sensitive nature of the observations and findings.

2.1 Description of tasking and sub- tasking activities

This secondary task element, as a function of the overall study methodology, is shown in figure 2 below. This is derived from the comprehensive Study Workflow as shown in Appendix A.

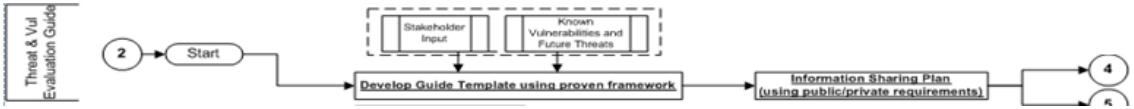


Figure 2 - Detailed workflow for Task 2

The core activities of this task involved the establishment of the technical committee comprised of partners, advisors, and subject matter experts specifically interested in addressing issues related to cyber threats and vulnerabilities within SCADA and control system environments. Like much of the tasking in the study, the activities in phase 2 of the project were done concurrently. As expected, the interdependencies between subtasks were substantial, and the study team cross correlated findings wherever possible. Fortunately, the approach used by the study team resulted in findings that accelerated a better understanding of the relationship between threats and vulnerabilities, and determined viable approaches to information sharing that address the security and privacy concerns of private sector asset owners.

Both the SCADA Cyber-Threat Working Group (SCTWG) and the SCADA Vulnerability Working Group (SVWG) were created at the onset of the tasking to define specific areas of focus that would prove most valuable to the stakeholder community. Wherever possible, these working groups were comprised of representation from the research, academic, asset owner, and public sector communities. The study team mandated a requirement that each member of the working group must, in some capacity, have technical experience as well as experience in managing cyber security issues within industrial automation environments. Time constraints, combined with seasonal holidays and the unfortunate withdrawal by some in-kind partners, forced the working groups to be ad hoc in nature. However, the study team repeatedly called on the expertise from this panel of experts and used their insights at various times during the tasking.

As the workflow indicates, concurrent activities of collecting stakeholder input and assessing both known vulnerabilities and future threats held populate a guide template. The study team perform exhaustive analysis of known SCADA vulnerabilities, as well as vulnerabilities not in the public domain, and use them to extract intelligence about future trending. It was well understood that a tactical information sharing plan would be critical in addressing private sector concerns, and pre-existing work was leveraged via the analysis of existing information sharing Memorandum s of Understanding (MoU's).

Approach to Subtask 2.1: *Develop and incorporate a SCADA cyber-threat matrix in consultation with critical infrastructure owners or operators, law enforcement, and the intelligence community.*

The key deliverable for Task 2 is the creation of a cyber threat and vulnerability evaluation guide for SCADA systems. It comprises the elements of subtasks 2.1, 2.2 and 2.3, which are, respectively: a threat matrix; a review of known vulnerabilities in SCADA systems; and the identification of approaches for addressing privacy concerns of private sector stakeholders for sharing threat and vulnerability reports with parties representing security interests within the Government of Canada.

The approach to the evaluation guide drew upon established information security audit and evaluation standards and methodologies as a means to ensure consistency with, and adaptability to existing security and risk frameworks in use throughout the private and public sectors. However, the level of process maturity in the stakeholder community with regard to security risk evaluation process was not consistent across sectors. Organizations with sophisticated IT governance frameworks and processes in many cases had not adapted them to the control systems domain. Therefore, to provide a consistent framework for evaluating threats and vulnerabilities to stakeholders, methods from organizations found to have

the most mature governance processes have been adapted as a means to meet their needs and in anticipation of the future needs and requirements from less mature organizations as they develop more formal security and risk management objectives.
To achieve this, the study has adapted components of the Harmonized Threat Risk Assessment (HTRA) methodology from Communications Security Establishment Canada (CSEC), which brings together security and risk assessment techniques from the RCMP and formerly CSE. Since the methodology is in use within the Government of Canada, and has been adapted in different forms in the provinces and within private sector organizations, this Threat and Vulnerability Evaluation Guide is intended to be both a lean evaluation framework for private sector organizations and to be compatible as a plug-in methodology component to the HTRA.
As a part of the development of the cyber threat and vulnerability evaluation guide for SCADA systems a cyber-threat matrix was derived from the classes and subtypes of threat agents assessed as a part of the HTRA methodology based on interactions with the stakeholders identified in the tasking.
The example threat scenarios are aggregations and variations on circumstances which evaluators have encountered in the field. They are intended to illustrate the capability of the threat agents to which SCADA systems and critical infrastructure have historic and current exposure and to note the level of apprehension of the threat by asset owners at the time of this report.

Approach to Subtask 2.2: *Develop and incorporate a review of the known vulnerabilities of SCADA systems, and project future threats and vulnerabilities to provide direction to future research areas*

An extensive review of available information pertaining to the current vulnerability landscape for SCADA systems was performed. The study team used material from several in-kind support partners as well as information derived from the vulnerability database created from their own research. In addition, the study team analyzed vulnerabilities that were discovered during the course of assessment projects and incorporated those findings into the study.[15] The SVWG members that could maintain continuous participation effort were also asked to contribute, where possible, and provide information for any vulnerabilities not found in the open source. To complement the analysis of vulnerabilities of SCADA systems, the study team also reviewed a comprehensive set of security incidents specific to industrial automation to gain a better understanding of the impact of these vulnerabilities when exploited by either intentional or unintentional threats.
The study team focused their analysis efforts on determining how to best categorize similar characteristics across the entire vulnerability landscape. As the project tasking involved the development of the framework for a threat and vulnerability evaluation guide, it was determined that having a comprehensive analysis of vulnerability types had a much higher value proposition than simply listing the vulnerabilities. As the study team had determined that since the reuse of the Threat Risk Assessment process was the optimum choice for a framework, continuing analysis as it pertains to consequence was very important. The study team also chose to interact directly with the stakeholder community once those vulnerabilities were analyzed, and used the collected information to assign priority to vulnerabilities and vulnerability type based on stakeholder perception.
The study team used numerous open source databases for the collection and analysis of vulnerabilities specific to SCADA. The study team extended their analysis to include vulnerabilities that were not necessarily SCADA specific, but were of a nature that if compromised could facilitate an adversary in causing impact to control system cyber operations. The resources leveraged in this task included material from:

[15] Vulnerabilities discovered during the course of regular study team activities are not found in the public domain as the activities related to coordinated disclosure have yet to be completed.

NIST/DHS National Vulnerability Database and primary resource feeds
DHS US-CERT
DHS Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT)
The Repository for Industrial Security Incidents (RISI)
Mitre , Vulnerabilities and Exposure (CVE)
Carnegie Mellon Computer Emergency Response Team/Coordination Center (CERT/CC)
The study team also investigated known vulnerabilities that were not control system specific in nature but would lead to a degradation in the security health of the control system should they be used. This analysis included vulnerabilities in operating systems and third-party applications, and focused on those that were found to be common within SCADA and control system and environments. Although it was expected that the review of known vulnerabilities of SCADA systems would provide for interesting results, the study team felt that such an analysis would be too narrow in scope. To facilitate for an accurate projection of future threats and vulnerabilities, as well as provide effective directions for future research areas, the study team also reviewed current offerings of vulnerability exploit frameworks and assessed how these frameworks are maturing as it pertains to control system cyber security (namely Metasploit, Immunity CANVAS, and Core Impact).

Approach to Subtask 2.3: *Identify various approaches to address the privacy concerns of private sector owners or operators in view of sharing cyber-threat and vulnerability reports with the CoPs and the federal government.*

Effective information sharing is critical to ensuring both private and public sector organizations have the necessary information to protect critical national infrastructure assets. Since the study team had extensive experience in working directly with critical infrastructure asset owners, key areas of concern regarding information sharing and disclosure of cyber incidents had already been identified. In addition, several members of the study team had previously been involved in the development of frameworks and information exchange portals specifically designed to facilitate information sharing between private sector asset owners and federal governments. These activities also had a specific goal of taking participant privacy concerns into consideration. The study team participated in several information gathering exchanges with project partners.
During the course of the study, Lofty Perch aggregated findings from engagements with asset owners and operators to determine the classes of threats and vulnerabilities to which their infrastructure was exposed. The evaluation guide divides threats and vulnerabilities into higher-order classes and subtypes, which enables asset owners and operators to aggregate their local concerns to ensure both the consistency and completeness of their cyber risk analysis.
The key technique was to segregate areas of technical and operational SCADA vulnerability from threats and risks so that the sensitivity of findings could be evaluated first against internal stakeholder operational concerns, and then separately against their impact on the broader critical infrastructure.

The approach to this subtask was to extract as much information as possible regarding the concerns shared across the private sector community. The subtask intended to determine what is required to exchange information regarding cyber-threat and vulnerability reporting in a manner that supports the privacy and security of the private sector entity. To enhance the value of the report findings, the study team elected to append this information with specific concerns the stakeholder community has about sharing their own incident information with the federal

government. This would ensure that the report contained information that encompassed all key areas pertaining to information sharing and could possibly lead to future study areas.

The study team evaluated perspectives from corporate and provincial privacy officers, and this was done to assess any emerging unique strategies that could support study goals.

2.2 Findings and observations

Subtask 2.1: Develop a SCADA cyber-threat matrix in consultation with critical infrastructure owners or operators, law enforcement, and the intelligence community.

The SCADA security threats perceived by asset owners and operators are IT security related threats from hackers, rogue employees, and in rare cases, sabotage from political pressure groups. Strategic national security threats affecting critical infrastructure are not a part of normal business and operational planning.

A class of advanced persistent threat (APT), as exemplified by Stuxnet, is being managed actively by asset owners via their IT security controls and programs. While the assets affected are SCADA control systems, the awareness and sources of control objectives originate in the IT security departments of the organization, and less often in the engineering and operations departments who manage SCADA systems.

Based on interactions with asset owners, the APT is perceived as being from "hackers" and the various motivations of virus and worm developers are viewed as tactical and unrelated to the specific business of the asset owner, and the threats are not typically viewed in the context of their potential strategic impact on the national critical infrastructure.

The key finding from the Threat Matrix exercise is that stakeholders should develop requirements for a comprehensive survey to collect information related to their specific objectives.

Subtask 2.2: Review known vulnerabilities of SCADA systems, and project future threats and vulnerabilities to provide direction to future research areas

The study analyzed roughly 240 known vulnerabilities specific to industrial automation, approximately 35 non-public vulnerabilities found by the study team, and more than 250 non-SCADA specific vulnerabilities that could impact the security of a control system. The analysis was comprehensive and included information available from the first quarter of 2005 up to and including the beginning of the third quarter 2011. The review included vulnerabilities specific to more than 65 vendor technologies. To complement the analysis of these vulnerabilities the study team also reviewed 60 confirmed malware incidents that occurred between 1982 and 2010 and assessed the vulnerabilities related to those malware incidents.

The study team selected the National Vulnerability Database (NVD) as the primary repository for vulnerability information. As this repository is centralized and contributed to by numerous other databases, metrics from it should be generally indicative of trending.[16] Analysis indicates that the

[16] The NVD was also selected to simplify any independent research activity the reader wishes to perform.

current rate of disclosure for security vulnerabilities that are specific to industrial control systems (and are submitted to the NVD via any number of formal vectors) is rapidly increasing. During the research period the study team reviewed roughly 110 vulnerabilities recognized by the NVD, with more than 50% of all control system vulnerabilities reported in the first two quarters of 2011.

The NVD was not the only source for information used in the study. At the time of this report there were in excess of 130 vulnerabilities analyzed that were specific to industrial automation but not contained within the NVD.

The study team evaluated known security vulnerabilities that are not control system specific but can impact the security posture of a control system. This analysis included operating systems, network devices, and third-party applications. The study showed that vulnerabilities that can potentially affect control systems are significant. Moreover, research and development in the control system cyber-security domain indicates that the increasing number of attack vectors used to compromise a control system is very similar to those used in traditional IT architectures. This observation, along with the obvious growth in interest regarding control system security, suggests that the control system vendor's dependence on third-party operating systems and applications may have a considerable impact on the security of SCADA systems. Collaboration with project partners, especially those in the asset owner and vendor community, suggests that the stakeholders are very concerned about not being able to secure the operating systems and applications upon which their critical cyber-assets are highly dependent.

The study was able to show that a considerable number of vulnerabilities that are not control system specific continue to impact the cyber security risk profile of control system environments. The rapid modernization and maturity of control system solutions, combined with the rapid rate of integration of commercial off-the-shelf operating systems and third-party applications, suggests that the severity of the impact on a control system cyber-security profile is increasing. An analysis of the vulnerabilities that are specific to control systems, when cross correlated with the research methods used for the discovery of those vulnerabilities, suggest that future adversarial tactics may include traditional IT attack vectors that compromise the underlying operating systems or applications. Once a compromise has been achieved, the trust relationship between underlying operating systems and the SCADA applications is simply leveraged to facilitate for unauthorized administrative access to the control system.

The review of vulnerabilities was to support the development of a framework for a cyber-threat and vulnerability evaluation guide, and the study team selected to categorize vulnerability attributes in a manner that can ease the complexity associated with calculating cyber-risk. As the study team had selected a pre-existing framework in the HTRA, it was most appropriate to look at vulnerability characteristics from the perspective of confidentiality, integrity, and availability. These can provide insight with regards to the level of effort required by the adversary to exploit the vulnerability and will plug directly into the matrices developed here and in other components of the tasking. This approach can then provide some direction in evaluating specific system risk as it pertains to the elements of threat and vulnerability.

The analysis demonstrated the majority of known vulnerabilities that are specific to industrial control systems impact the system 'availability' attribute. It is generally agreed upon that confidentiality is the most critical security requirement in IT systems, followed by integrity and availability (in that order). Contrary to this, availability is the most critical security requirement in the SCADA and control system domain. This primary requirement is followed by integrity and confidentiality Research has shown that this perspective is accurate as critical infrastructure systems have extensive availability requirements followed closely by the requirement for sound operational data (integrity). As such, if availability is a primary requirement from a control system security perspective then the fact that a majority of the known vulnerabilities impact system availability is concerning.

Vulnerabilities and SCADA System Availability

A review of the more than 240 known vulnerabilities specific to control systems indicates that approximately 132 (55%) may result in denial of service when exploited. Of the 35 non-public vulnerabilities (as derived from the study team's independent research during assessment activities) 20 (57%) result in denial of service (DoS). The analysis regarding compromise of availability can be extended, as the study showed that in addition to those vulnerabilities specifically resulting in a compromise of availability the vulnerabilities that lead to system compromise can indirectly lead to total system control should adversary choose to impact the system that way.

To facilitate the alignment of vulnerabilities with threat and consequence, the study team determined that the common denial of service vulnerabilities resulted from:

Improper bounds checking for data inputs, resulting in buffer overflows that can be used to write into random or specific memory space
Improper session management leading to a uncontrollable unmanaged connection states
Factory deployed emergency shutdown capability, allowing for shutdown or reboot once an undocumented password is used
Default reboot protocol, allowing an attacker to force system reboots ad infinitum
Memory leaks on physical devices creating opportunities for extensive resource consumption
Embedded diagnostic utilities that can create resource consumption failures when activated during normal system operation (on-line)
Heap buffer overflows resulting in denial of service when excessively long data strings are submitted following valid packet streams
Unauthorized access to embedded device Web servers allowing for an adversary to set refresh rates so high it renders the user interface inoperable
Critical devices vulnerable to loading and executing corrupted firmware, resulting in a system malfunction and denial of service
Inappropriately programmed field equipment forced into sending bulk multicast network subscription messaging, thus flooding the network and preventing normal control communications
Various buffer overflow vulnerabilities resulting in the corruption (and non-functioning) of embedded device web pages and remote connection services (ftp, telnet, rsh etc)
Various instances of NULL pointer dereferencing
Denial of service due to performance failures from service scans and enumeration, some resulting in system auto-restore to factory settings (and thus being rendered unusable in a production environment)

Vulnerabilities and SCADA System Integrity

A review of the more than 240 known vulnerabilities that are specific to control systems indicates that approximately 84 (35%) may facilitate for an attacker to either modify data related to the operation of the control system or compromise the system to the point of assuming administrative privileges. Of the 35 non-public vulnerabilities (as derived from the study teams independent research during assessment activities) 10 (29%) can result in modification of system data or privilege escalation. The analysis regarding compromise of integrity can be extended. The study showed that in addition to those vulnerabilities that can specifically result in a compromise of integrity, the same vulnerabilities may lead to total system compromise and allow the adversary free will to control the system at will.

To facilitate realignment of vulnerabilities with threat and consequence, the study team determined that the common integrity vulnerabilities resulted from:

Improper bounds checking for data inputs, resulting in buffer overflows that can be used to write into random or specific memory space and resulted in the creation of new users or the execution of arbitrary code

Hard-coded and/or known default passwords used for system administration

Inappropriate use of least privilege practices, allowing an attacker to exploit one system application to gain access into more authoritative ones

Embedded web services vulnerable to cross site scripting

Unrestricted file content uploads and no destination bounds checking

Various database and SQL injection vulnerabilities resulting in modification of operational data or creation unauthorized (but privileged) users

Critical devices vulnerable to loading and executing modified firmware (with the intent to create new user accounts or remove credential requirements)

Lack of message authentication facilitating for various man-in-the-middle type of attacks

Various buffers overflow vulnerabilities resulting in the modification of embedded device web pages and authorized host listings

Vulnerabilities and SCADA System Confidentiality

The interpretation of what confidentiality means varies across the stakeholder community. The study team chose to define vulnerabilities related to confidentiality as those weaknesses that, if exploited, could result in the inappropriate disclosure of sensitive operational information possibly leading to a full compromise of the control system.

A review of the more than 240 known vulnerabilities specific to control systems indicates that approximately 24 (10%) may facilitate for an attacker to compromise aspects of confidentiality within a control system. Of the 35 non-public vulnerabilities (as derived from the study team independent research during assessment activities) 5 (14%) could result in access to system data that could be used to facilitate an attack. The analysis regarding compromise of confidentiality can be extended. The study showed that in addition to those vulnerabilities specifically resulting in a compromise of confidentiality, the same vulnerabilities can also be used to allow an adversary free will to control the system.

To facilitate realignment of vulnerabilities with threat and consequence, the study team determined that the common confidentiality vulnerabilities resulted from:

Plaintext communications between operator control environments and field devices, allowing for the extraction of credentials

Poor password obfuscation and client-side storage of authentication credentials

Unsecured directory traversal vulnerabilities

Unauthenticated acquisition of user and system configurations direct from field devices and operator consoles

The study was able to demonstrate that the current trending in the research and discovery of vulnerabilities that are specific to control systems directly follows the methodologies commensurate with traditional IT. Perhaps more importantly, analyses of the technical specifics of the known vulnerabilities suggest that the increasing dependence on common operating systems and third-party applications may have a negative impact on the cyber security posture of a SCADA system. The analyses of the technical specifics of the vulnerabilities that are not publicly known also align with this observation, and the discovery and verification of the vulnerabilities in the systems can also be done using traditional IT approaches. From this analysis it would appear that the landscape regarding control system vulnerabilities is in a very dynamic state, and although there appears to be a considerable increase in widespread interest of control system security vulnerabilities the most economical attack vectors may be associated with traditional IT security vulnerabilities. The study team explored this theory with both representation from the project SVWG and the stakeholder community and found that this is a sound assumption.

The study team also explored the status of current and emerging vulnerability exploit frameworks and found that there are no significant modifications to the operational specifics of the frameworks but that the datasets and composition of program modules are tuned to accommodate specific vulnerabilities within control system environments. From the perspective of building a defense posture, this is encouraging due to the fact that contemporary intrusion detection and prevention methodologies can be tuned to detect and mitigate attacks that leverage existing exploitation frameworks.

Although capable of being configured to account for the entire collection of known SCADA vulnerabilities, the commercially available versions of exploit frameworks currently contain roughly 15% of the modules that align with the open source vulnerabilities associated with industrial automation. The same frameworks account for almost 85% of the vulnerabilities that are not control system specific (but could impact the cyber risk profile of the control system), and 0% of the vulnerabilities known only to the study team (and are not in the public domain). The reader is

encouraged to research how contemporary vulnerability exploitation frameworks are being used in the control system domain, as an in-depth discussion and analysis is beyond the scope of this report.

Projection of Future Threats and Vulnerabilities

The study tasking required an analysis for the projection of future threats and vulnerabilities as they pertain to SCADA systems. The interactions with the stakeholder community indicate that the categorization of threats is nontrivial. Each stakeholder can define threat based on the sector in which they operate and the specific requirements of the industrial automation on which the business depends. To that end, the study team determined that the stakeholder community is interested in understanding what the future vulnerabilities will look like and will use that information to shape mitigation and countermeasure strategies to reduce overall cyber risk. The study team digested this requirement and determined that the projection of future vulnerabilities can be best accomplished by aligning characteristics of those vulnerabilities with plausible attributes of future threats.

The results from the study indicated that threat actors will continue to be defined as either direct or indirect, and will continue to leverage open source consequences that were either driven by deliberate or accidental actions. In either case, vulnerabilities will continue to be seen in both direct and indirect actions, but it can be expected there will be a noticeable increase of deliberate (direct) attacks using vulnerabilities that are specific to control systems. At the time of report generation, security activities that relate to the development of Stuxnet-like malware are already starting to surface, suggesting that the landscape of adversarial awareness has changed and the attention to SCADA cyber security has increased.

The analysis also suggests that there may be no reduction in reports of control systems being impacted by viruses and malware. In addition, the growing dependence that SCADA has on common operating systems and third-party applications will result in more control systems being impacted by hostile mobile code, code that may not have been developed specifically for industrial automation. The analysis of repositories specializing in the collection and review of control system security incidents supports this projection, suggesting that future research areas also include extensive analysis of how vulnerabilities within common operating systems and applications can impact SCADA security.

The rapidly developing capabilities of industrial automation, combined with the increasing number of user configurable services and aftermarket support for third-party applications, draws attention to the security issues related to the asset owner procurement chain or the supply chain of the vendor. Numerous reports of incidents involving a compromised supply chain suggest that security profiles of control systems could be negatively impacted during the development phase of the system itself. Analysis suggests that the access vectors into either the supply chain or the procurement process facilitate for a wide range of plausible attack vectors an adversary could use to compromise the system. More importantly, this compromise could occur anywhere in the system development lifecycle or in the development lifecycle of solution elements beyond control of the original equipment manufacturer.

The vulnerabilities associated with supply and procurement chain operations can be categorized in a similar fashion to those vulnerabilities that are already known. However, it is entirely plausible that derivatives of well-known vulnerabilities in SCADA systems can be used to develop unknown vulnerabilities, thus empowering an adversary to create exploit mechanisms to which there may be no defense (i.e. 0-day vulnerabilities). When the class or category of threat agent is taken into consideration, combined with whether or not the attack is deliberate or unintentional, a significant number of plausible consequences can be developed. This modeling can also take into consideration the sector in which the attack happens. Vulnerabilities that can be dormant until activated by an adversary, especially ones that can go undetected and are deployed during the system development process, may present the greatest level of irreducible uncertainty and risk. Furthermore, these types of attacks and vulnerabilities have been observed and indicate extensive involvement from actors most likely operating at a nation state level.

The study team worked with their partners to ascertain how the growing rate of SCADA vulnerabilities can alter the way adversaries approach critical infrastructure. Analysis suggests that the vulnerabilities specific to industrial automation can correlate to the traditional IT vulnerabilities. However, trending indicates that there is an emerging interest in expanding traditional low/medium impact attack methodologies to activities that exploit specific SCADA vulnerabilities in an attempt to trigger kinetic (real world) events. As such, it can be projected that future SCADA vulnerabilities may be discovered and exploited to empower an adversary to have complete command and control over the critical process.

The study also showed that one of the more complex issues in understanding control system vulnerabilities is that many of the 'perceived' security vulnerabilities are actually system administrator functions that, if abused by an adversary, would empower the adversary to operate the system as any rogue (but authorized) insider operator. It was this observation that allowed the study team to project that notable SCADA vulnerabilities of the future could correspond to positioning the attacker in an extremely privileged role. To that end, these vulnerabilities may be specific to the exploitation of security shortcomings with in customized control system programs or the exploitation of undocumented (or accidental) system functions.

Future Research Directions

The extensive work done by the study team in reviewing known vulnerabilities of SCADA systems, combined with an analysis of pertinent vulnerabilities that were not control system specific, facilitates for excellent analysis on what directions are needed for future research. More importantly, as the study team was able to incorporate their own findings (from independent research that was happening concurrent with the study activities) the study team is well-positioned to provide insight that has immediate applicability.

During the course of the tasking, the study team was able to determine an extensive set of ideas that could be used to help guide future research directions in SCADA security. The study results indicated that although there are several research domains of interest that could prove useful, feedback from the project partners and stakeholder community suggested that research that results in a better understanding of adversarial activities (and how to counter those activities) would be most beneficial. The study team found this approach sound, as it was determined that existing recommended best practices in SCADA security could provide for a solid framework for future research directions. Not only is this approach in line with stakeholder expectations it is the most economical, as it can be situated as an overlay upon current research activity and threat/risk standards being done within the government, academic, and asset owner domains.

The community of interest could benefit from a better understanding of how adversaries are either using or planning to use exploit frameworks in their attacks. Although current market-leading exploit frameworks embed roughly 36 (15% of 240) of the known control system vulnerabilities, for the 'medium to advanced' adversary the incorporation of SCADA-specific security weaknesses into these frameworks may be trivial. During the tasking, the study team was able to easily understand the process associated with building exploit modules for these frameworks so that they would target specific control system environments and exploit specific vulnerabilities. Although the current research indicates that this type of activity is not widespread, research efforts seeking to understand why this is the case could provide useful intelligence towards building effective countermeasures.

The research results pertaining to how exploit frameworks can be used against control system environments can also create anomaly detection signatures. This can provide asset owners with better information on how to customize security countermeasures that are specific to their industrial automation environments. This research could be extended to facilitate for a better understanding of the customization of intrusion detection

systems to defend against exploit frameworks using unknown or ‘zero-day’ vulnerabilities specific to SCADA. It would be a very interesting exercise to develop the security modules for all 250 known SCADA-specific security vulnerabilities, and assess the value proposition that such a complete set of modules would have to the stakeholder community. This information could also be used to support law enforcement and intelligence community efforts as it pertains to the location and aggregation of open-source information, as well as provide for more successful interactions with the stakeholder community.

Collaboration with the stakeholder and project partners indicated that the concerns regarding the security of products and services within a procurement or supply chain are increasing. The study team was unable to collect any information on current or emerging technical solutions to address this problem. Organizations are beginning to develop policy and assessment procedures to gain clarity on the security posture of OEM technology, but these procedures are paper-based and rely on vendor answers to simple questionnaires. The fact that there can be hundreds (if not thousands) of procurement/supply chain elements involved in the creation of a single product makes the comprehensive security analysis of SCADA solutions complicated at best. Future research activities that can help an asset owner or vendor perform technical and non-technical security reviews on solution elements would be very useful. This research should include effective approaches to assessing the security profiles of operating systems and third-party applications, and investigate the requirements necessary for an asset owner to appropriately qualify risk as it pertains to critical assets. This, in turn, will empower the asset owner to create appropriate security countermeasures that accommodate for both the uniqueness of their operational environment and any inherent security vulnerabilities that may exist in constituent technology over which they have no control.

One of the more interesting reoccurring discussions that took place between the study team and stakeholders, particularly those from the vendor community, was that although SCADA technology is uniquely tuned for each specific customer there are elements of the solution that are ubiquitous across the entire vendor client base. This fact creates concern for how the discovery of a vendor specific vulnerability, one that could have applicability across a substantially large asset owner community, could provide an adversary with a mechanism to cause widespread negative impact. During the tasking, the study team found that a capability to monitor security health of critical SCADA systems that are not connected to each other, but share similar/identical OEM solutions, could provide valuable situational awareness. By having such a capability, countermeasures can be created to possibly trigger on specific adversarial activities against a community using common vulnerable systems. In tandem with research addressing how exploit frameworks can be modified and used against industrial automation environments, the intelligence collected by this capability would be very useful.

Effective mitigation strategies could also be improved upon by the results from research that provides insight on how to aggregate and analyze asset owner log and audit files in a manner that does not impact privacy but supports requirements to derive holistic views of the technical security health of national critical assets. Analysis of this research area indicates the inputs to the research project must not only come from the asset owner community but also the vendor, as it would be imperative that the advancements in research pertaining to understanding adversarial activities against the community using the same vulnerable systems are required. Input from the vendor would be mandatory to ensure useful results and reasonable strategies.

As the study team carried out their analysis regarding required research areas, some other concurrent activities in infrastructure protection and resiliency provided insight on another research area that could prove valuable to the Canadian stakeholder community. The assessment of known and unknown vulnerabilities in SCADA systems provides some very detailed information about how an adversary could impact or compromise a control system and the level of effort required to do so. By working with asset owners it should be straightforward to categorize the severity of consequences associated with sector specific operations. By reviewing the range of consequences, as well as adversarial methodologies required to

create those consequences, a cross correlation of the vulnerabilities can be used to define what the attacker methodology could actually look like.[17] The research opportunity then becomes one associated with developing a predictive analysis capability using the system or abilities in the development sector specific attack tree models. Currently, members of the study team are working on several sector-specific initiatives in this area but interactions with the stakeholder community suggest there are many opportunities to continue advancing this research in the sectors that are not currently being addressed.

The final opportunity for research is based on the fact that a majority of the vulnerabilities reviewed (both open source and non-public) has specific implications to both the electric and transportation sectors. From an analysis of the known security incidents that have impacted control system operations it was determined that those incidents that exploit known vulnerabilities are most common in these sectors, and the technology impacted is common to both. The study team has analyzed this information and determined that there is a substantial opportunity for SCADA security research that addresses issues in the distribution automation and transportation sectors.

Specifically, plausible future research areas include (but should not be limited to):

Security vulnerability assessments in Advanced Metering Infrastructure and Advanced Meter Reading (AMI/AMR)

Security vulnerability assessments in hardware and firmware solutions for power management systems

Cryptographic and security analysis of embedded systems used for long-range telemetry and radio communications

Security analysis of mobile ad hoc networking solutions used for integrated energy and transportation systems

Security analysis of mobile 3G/4G WiMax solutions for critical infrastructure data aggregation and management

Security analysis of contemporary process control solutions and their impact to environmental operations (HVAC)

The information that provides basis to these suggested research activities is sensitive in nature and is beyond the scope of this report. However, a detailed analysis of existing control system vulnerabilities and the observed level of research activity in certain sectors clearly indicate where research opportunities arise.

Subtask 2.3: Identify various approaches to address the privacy concerns of private sector owners or operators in view of sharing cyber-threat and vulnerability reports with the CoPs and the federal government.

Since the study team had extensive experience in working directly with critical infrastructure asset owners, key areas of concern regarding information sharing and disclosure of cyber incidents had already been identified. In addition, several members of the study team have previously been involved in the development of frameworks and information exchange portals specifically designed to facilitate information sharing between private sector asset owners and federal governments, with the specific goal of taking participant privacy concerns into consideration. The study team updated a pre-existing questionnaire to accommodate for the needs of the tasking and participated in several information gathering exchanges with project partners.

The approach to this subtask was to extract as much information as possible regarding the concerns shared across the private sector community, and how to exchange information regarding cyber-threat and vulnerability reporting in a manner that support the privacy and security of the entity. To enhance the value of the report findings, the study team elected to append this information with specific concerns the stakeholder

[17] Its simplest format, this analysis can be performed assuming that the adversary will use the most economical approach to system compromise.

community has about sharing their own incident information with the federal government. This would ensure that the report contained information that encompassed all key areas pertaining to information sharing and could lead to future study.

The study indicated that the majority of stakeholders understand the importance of reporting criminal activity to law enforcement. Many asset owners have extensive experience working with law enforcement regarding physical and personnel security and have been able to extend their operational protocol to include cyber. A majority of asset owners engaged for the study have not had the opportunity to communicate with law enforcement regarding SCADA security incidents, but there appears to be a fairly broad willingness to communicate with law enforcement when there is a perceived criminal aspect to the cyber incident.[18]

The study team interacted with representation from other national law enforcement and national security communities. As is the case in Canada, stakeholders recognize a clear delineation between law enforcement activities and national security activities pertaining to critical infrastructure and cyber security. Outreach campaigns around the world appear to be successful, as the law enforcement community is positioned very clearly as a tactical response arm supporting criminal investigations to the asset owner, while the national security function provides timely threat information to help asset owners proactively mitigate against possible adversarial activities. Regardless, the success of information sharing campaigns is entirely contingent on the ability and willingness of the asset owner to report security activity and receive useful intelligence products.

As clear as this might sound, the study observed discrepancies in how willing an entity may be in communicating with law enforcement or national security representation. The study indicated that because federal law enforcement representation may have a more advantageous proximity to the actual stakeholder (field offices), outreach campaigns may result in the establishment of more effective relationships. This is not to say that asset owners did not see value in the efforts by government representation located in a remote national capital, but the willingness to share security information seems to be correlated with the personal relationships that can be established between the government representative and the actual asset owner. This may suggest that some significant barriers have unintentionally been created between private sector and the federal government, and in turn these barriers have prevented effective information sharing between the private sector and any efforts sponsored by federal entities.

Fundamentally speaking, there were several areas of concern shared across the private sector community that may impact the readiness, willingness, and capability to contribute to security incident and information sharing programs sponsored by the Canadian federal government. These include:

The asset owner is unaware of any Canadian federal government information sharing programs addressing control systems and critical infrastructure protection

The asset owner is unsure of the Canadian federal government's technical capability to understand critical infrastructure systems impact, and as such cannot appreciate the value of any capability that can be used for incident submission or threat reporting

The asset owner does not have a formal or approved capability to share SCADA security incident information with anyone beyond the corporate entity

The asset owner has an information sharing capability but the restrictions are such that only sector peers and business partners are to be communicated with

The asset owner is required to only share security information with pre-existing sector specific information sharing portals and regulatory bodies

[18] It should be noted that this willingness amongst Canadian asset owners may be a direct result of the extensive outreach efforts demonstrated by the RCMP Technical Crime Unit and their commitment to holding an annual SCADA and Industrial Control Systems cyber security workshop specifically for Canadian asset owners.

The asset owner is not comfortable with the levels of information protection provided by the Canadian federal government
Concerned with information leakage to the media
Concerned with information leakage to other government departments
The asset owner is unaware as to which Canadian government entity should receive the information (and as such doesn't bother reporting)
The asset owner feels that the level of technical understanding by the Canadian national security and intelligence community is insufficient to appreciate the nature of the information

This list comprises some of the more important issues that need to be addressed, and clearly demonstrates an opportunity to describe various approaches to address the concerns of the private sector owners. These issues are not new to the Canadian federal government, and recent campaigns to mitigate these problems have begun. Progress in mitigating private sector concerns, especially those that relate to how private sector asset owners can get access to sensitive information resources, has been made. Recognizing the clear need to create mechanisms to collect private sector information as well as deliver sensitive threat data, numerous approaches have been developed and incorporated into information sharing agreements.

The development of information sharing agreements through memorandums of understanding appear to be the most appropriate way to address many or all of the concerns presented by the stakeholder community. Analysis of ongoing efforts indicates several common themes presented in information sharing agreements, including:

A clear and concise statement defining the need for the information sharing capability
A clear and concise statement defining the role of the government agency requesting an information exchange, and why they need to share information with the private sector
A clear and concise discussion of the mechanism used to facilitate the exchange of information
A clear and concise discussion of the benefit to the asset owner
A clear and concise discussion of the asset owner responsibilities associated with using the information sharing capability and data extracted from it, including any legal requirements mandating their actions
A clear and concise discussion of how the sponsoring government agency may use information submitted by the asset owner
A clear and concise statement defining how the government agency will mark, protect, and handle information submitted by the private sector entity
A clear and concise statement defining how the government agency will protect the information from inadvertent disclosure and requests under any Privacy Act or Access to Information Act and any mandatory disclosure requirements the information may be subject to

Currently, there exists several agreements (globally) that facilitate for effective public/private information exchange partnerships. As an example, the information made available to stakeholders through the RCMP Suspicious Incident Reporting (SIR) portal can be used by asset owners to better understand risk. The RCMP has created a Memorandum of Understanding template that private sector critical infrastructure stakeholders must sign in order to get access to the SIR information sharing portal. The MoU is now defined as a User Access Agreement and facilitates access to the portal to report incidents that are not clearly criminal in nature but suspicious (and hence worthy of reporting). This MoU agreement has been provided in Appendix B, and should be reviewed by the reader in the context of being a plausible framework for information sharing initiatives that address the more salient concerns of the stakeholder community.

During the tasking, the study team engaged with provincial privacy commissioners to discuss their perspectives of privacy requirements for critical infrastructure asset owners. Information collected from these discussions indicated that the current focus of the privacy community, at least at the provincial level, is towards requirements that address the needs of individual citizens as opposed to those in large asset owner environments. Although there was no disagreement with regards to the importance of protecting personally identifiable information, there is still much opportunity for discussion as it pertains to the protection of corporate privacy information when security incident or threat data is to be exchanged. This suggests the work done by the federal government in developing memorandums of understanding is probably the most appropriate starting point.

The approach that is currently used by the RCMP, as well as similar approaches used elsewhere, may not be enough to facilitate for a comprehensive enrollment from all asset owners across the country. During the tasking, the study team explored data classifications and categorizations that could be used to enhance the protection of sensitive critical infrastructure information. Specifically, the work that is being done by the United States Department of Homeland Security pertaining to the classification of Protected Critical Infrastructure Information (PCII) should be perceived as a benchmark for categorizing sensitive private sector information. Information that is categorized or classified as PCII is exempt from requests made using any privacy or access to information request. Analysis shows that private sector organizations that are able to have their information categorized under PCII are exceptionally comfortable with releasing that information to the federal government and tend to be more willing to share (either supply or receive) sensitive security incident information with the federal government.

Currently, however, the existing memorandums of understanding that have been developed for information sharing provide a very good foundation for future information sharing strategies. Further research in this area could be directed towards the analysis of how any sector specific information sharing portals have been successful. The study team investigated this and determined that this is worthy of future analysis, as many of the successful information sharing portals that are sponsored by the federal government do not facilitate for the federal government to have access to private sector security information.

2.3 Cyber threat and vulnerability evaluation guide

Identification of shared risk through a common assessment framework will support the alignment of the security interests of stakeholders.

The cyber threat and vulnerability evaluation guide comprises a set of appendices which are adapted from the RCMP/CSEC Harmonized TRA Methodology. The subset of TRA artifacts was selected to narrow the focus to SCADA systems and assets with exposure to logical/kinetic interfaces. The artifacts are intended as a framework to provide clear definition of scope, while preserving the value derived from the threat and vulnerability assessment exercises. By executing an assessment based on the guide, the results will be compatible with existing risk management frameworks within the federal and provincial governments, as a means to facilitate information sharing between the private public sectors, and to provide an objective view of the risk factors facing SCADA systems.

The guide enables a foundation for a common understanding of how threats, vulnerabilities and risks to cyber and SCADA systems may be expressed and communicated between diverse stakeholders across public and private sectors. This basis for articulating shared cyber risk is necessary to facilitate the stated objective of threat and vulnerability information exchange.

The components of the HTRA methodology which have been adapted for this plug-in SCADA evaluation guide include the following:

Appendix C Sample Statement of Work: A guide for structuring a cyber threat and vulnerability evaluation engagement based on the HTRA methodology.
Appendix D Cyber Controls Systems Asset Listing: A list of assets that define the scope of the assessment and which may be vulnerable to threats.
Appendix E Asset Valuation and Sensitivity: Classes and subtypes of assets to determine the scope of the evaluation engagement and the sensitivity of the assets to a compromise of the asset related to data confidentiality, data and system integrity, data and system availability and physical safety as a result of system failures.
Appendix F Threat List: Classes and subtypes of threat agents
Appendix G Threat Assessment: A table with examples as a guide for listing threats and assessing their impact in the event of the exploitation of vulnerability related to an asset.
Appendix H Vulnerability and Risk Sources: A table for enumerating areas of vulnerability and recording the perceived the likelihood and impact of vulnerability being exploited, or of a safeguard or control process failing.

These components meet the subtask requirements according to the following table.

	In Support of Subtask		
	2.1 Threat Matrix	2.2 Known Vulnerabilities & Future Threats	2.3 Information Sharing Approaches
Evaluation Guide Document			
Sample Statement of Work		☐	
Cyber Control Systems Asset Listing			☐
Asset Valuation and Sensitivity	☐		☐
Threat List	☐		
Threat Assessment	☐	☐	☐
Vulnerability & Risk Sources			☐
Threat Matrix	☐	☐	☐

Figure 3 – Evaluation Guide Documents to Subtasks for Task 2

2.4 Conclusions

The evaluation guide is designed to assess threats, vulnerabilities and risks. After an assessment based on the guide has been completed and the residual risks have been identified in the private sector, stakeholder concerns about *threats* and *threat agents* may be shared with the federal government for management and mitigation, particularly without the implications of fault or vulnerability.

A possible approach would be to promote a risk evaluation guide to stakeholders with the offer of assistance in regard to mitigating specific threats once they have determined the risks for themselves.

A key message is to differentiate vulnerability from threats and risks. As an approach to greater engagement between government and asset owners and operators, stakeholders must be educated about the difference between technical vulnerabilities and threats so that the asset owners and operators may be able to provide more precise information about security threats and risks, without incurring business-cost risk from courting regulatory scrutiny of perceived deficiencies.

The focus on technical vulnerability provides "low hanging fruit" for producing new security intelligence since the information is verifiable, and presents fewer challenges to relationships with parties who may object to being classified as a "threat" or a source of risk. However, the technical vulnerability landscape changes daily, sometimes hourly, with the publication and refinement of vulnerability information evolving mostly from collaborative "crowd sourced" efforts on the internet. The collection and development of information about technical vulnerabilities is a class of problem suited to task-specific organizations that can retain the dynamic specialist expertise for point in time analysis, and which can limit their accountabilities to task-based deliverables, all without the overhead of maintaining complex relationships with governments, civil society and interest groups, media and other parties.

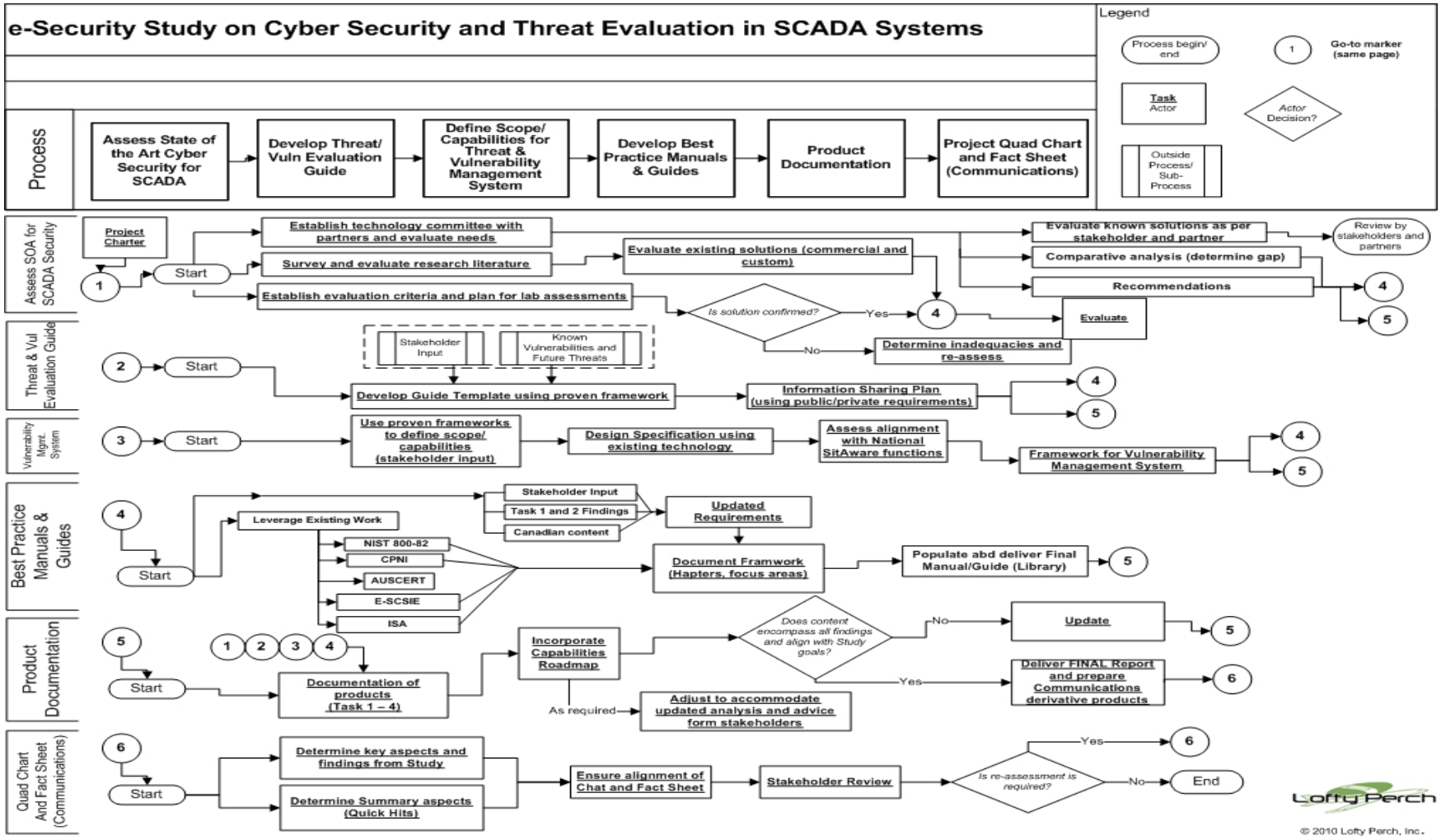
For most asset owners and operators, technical vulnerability information about their infrastructure and operations is considered sensitive and it was not clear from interactions with them what benefits compensate them for costs and risks from collecting or producing and disclosing the information.

In engaging private stakeholders, public sector agencies might de-emphasize the focus on individual areas of technical vulnerability in private sector stakeholder systems and operations, which are interpreted (accurately or not) as faults in the organization and in turn expose the organization to risk from being made an example of via regulatory, political or legal intervention.

A better understanding of the risks from disclosing technical vulnerability information to a specific government department is required before a persuasive case for disclosing it can be made. Since disclosures are at this point hypothetical, it is not known how the information might be used, how it would be protected, and again, how providers would be compensated for the resources required to collect it.

A plan that supports a broader critical infrastructure security strategy to accomplish national security objectives would provide a foundation for stakeholder engagement from the asset owner and operator community, which would in turn enable the derivation of clear information requirements. These requirements should drive the adoption of practices for information sharing, since without requirements, it is difficult to evaluate the quality and effectiveness of any effort made toward their implementation.

Annex D Project workflow



Annex E Sample Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

THIS ARRANGEMENT, made in duplicate as of the day of 2011

BETWEEN

THE ROYAL CANADIAN MOUNTED POLICE
(HEREINAFTER REFERRED TO AS "RCMP")

AND

CI STAKEHOLDER
(HEREINAFTER REFERRED TO AS THE "CI Stakeholder")

BACKGROUND

WHEREAS Critical Infrastructure Protection is recognized as an essential element to Canada's national security;

AND WHEREAS the aforesaid recognition of Critical Infrastructure Protection is addressed in, among other places, the Emergency Management Framework for Canada, the Government of Canada's *Emergency Management Act*, the National Strategy for Critical Infrastructure, and the Action Plan for Critical Infrastructure;

AND WHEREAS information sharing and information protection among CI Stakeholders and the Government of Canada and its Critical Infrastructure security partners including the RCMP are recognized as important elements of Critical Infrastructure Protection;

AND WHEREAS the Government of Canada's *Emergency Management Act*, which came into force in 2007, includes a consequential amendment to the *Access to Information Act* to give additional protection to certain types of sensitive information.

AND WHEREAS the RCMP has a mandate to collect information on criminal threats against Critical Infrastructure to improve Critical Infrastructure Protection;

AND WHEREAS information sharing between all CI Stakeholders concerning threats to Critical Infrastructure is essential to improve Critical Infrastructure Protection;

AND WHEREAS the Critical Infrastructure Criminal Intelligence (CICI) section has a lead role within the RCMP's National Security Criminal Investigations (NSCI) branch to collect information concerning all potential criminal threats to Critical Infrastructure;

AND WHEREAS the RCMP has developed a secure portal, known as the Suspicious Incident Reporting (SIR) system, to collect information on suspicious incidents related to Critical Infrastructures and to disseminate criminal intelligence assessment on potential criminal threats to Critical Infrastructure;

NOW THEREFORE THE PARTICIPANTS INTEND AS FOLLOWS:

1. DEFINITIONS

"Critical Infrastructure" means the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical Infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders;

"CI Stakeholders" are all private and public organizations that have a role and responsibility in ensuring the security and/or continued operation of assets that are part of Canada's Critical Infrastructure;

"Critical Infrastructure Protection" means the protection of Critical Infrastructure.

"Participants" means the RCMP and the CI Stakeholder;

"SIR" means the secure portal developed and maintained by the RCMP where SIR Reports can be submitted and criminal intelligence assessments can be extracted. The system will evolve on a continual basis and the specific information technology used to implement the secure portal is

subject to change over time;

“SIR Information” means all information that is submitted to or extracted from the SIR;

“SIR Report” means a report concerning a suspicious incident that could indicate the existence of a potential criminal threat to Critical Infrastructure inputted into the SIR by a CI Stakeholder;

“SIR Users” means employee(s) or contractor(s) of the CI Stakeholder whose duties require access to the SIR and who have been security cleared to a LEVEL-II SECRET Government of Canada security clearance and a supplemental RCMP database verification;

“MOU” means Memorandum of Understanding.

2. PURPOSE AND SCOPE

2.1 The purpose of this MOU is to enhance Critical Infrastructure Protection by sharing information concerning potential criminal threats to Critical Infrastructure through the SIR.

2.2 This MOU sets out the roles and responsibilities of the Participants concerning the submission of SIR Reports to the SIR, access to the SIR, and the Participants’ obligations with respect to SIR Information.

3. SUSPICIOUS INCIDENT REPORTS

3.1 Subject to applicable laws, the CI Stakeholder is expected to submit SIR Reports on suspicious incidents that could indicate a possible criminal threat to Critical Infrastructure. The CI Stakeholder understands that while there is no legal requirement to report suspicious incidents to the SIR, such information can be crucial in identifying potential criminal threats to Critical Infrastructure.

3.2 The CI Stakeholder understands that in the event that any incident or threat requires an immediate police response, the CI Stakeholder should contact the police of local jurisdiction through the appropriate emergency channels. The CI Stakeholder also understands that the purpose of the SIR is to gather information on potential criminal threats to Critical Infrastructure, and not to enable a law enforcement response for a specific incident.

3.3 The CI Stakeholder understands that it is their responsibility to ensure the security of their assets. The CI Stakeholder also understands that the SIR will support their efforts to secure their assets by providing criminal intelligence assessments on potential criminal threats to Critical Infrastructure.

3.4 The CI Stakeholder understands that the RCMP is not responsible for responding to specific incidents reported on the SIR. The CI Stakeholder also understands that the RCMP may forward SIR Information to the police of local jurisdiction and/or take appropriate follow up action as deemed necessary.

3.5 The CI Stakeholder understands that the RCMP may share any SIR Information with the Canadian Security and Intelligence Service (CSIS) for purposes of fulfilling its mandate in relation to national security.

3.6 The CI Stakeholder may share a SIR Report with the police of local jurisdiction, subject to explicitly indicating, in its submission to the SIR, its intention to share the SIR Report with the police.

3.7 The CI Stakeholder may share a SIR Report, vetted by the RCMP to not contain any personal information, with a Federal Government department or agency, subject to explicitly indicating, in its submission to the SIR, its intention to share the SIR Report with the Federal Government department or agency, and further subject to the Federal Government department or agency having:

(a) signed an information sharing MOU with the RCMP with respect to access to the SIR; and
(b) a lawful mandate to receive the SIR Information.

3.8 The RCMP will provide the CI Stakeholder with assessments about potential criminal threats to Critical Infrastructure, based on the SIR Reports received and other available sources of information. The assessments will not disclose specific vulnerabilities or proprietary information of any of the Participants.

3.9 The Participants acknowledge that there is no intention under this MOU to collect personal information.

4. CONFIDENTIALITY AND USE OF INFORMATION

The CI Stakeholder intends to:

4.1 use the SIR Information solely for the purpose of Critical Infrastructure Protection;

4.2 take all reasonable measures to preserve the confidentiality and integrity of the SIR Information against accidental or unauthorized access, use or disclosure;

4.3 treat SIR Information in accordance with the security markings on it and to provide equivalent protection to it while it is in its possession;

4.4 abide by all caveats, conditions or terms attached to the information received from the SIR and follow the need to know principle;

4.5 refrain from sharing any SIR Information with any third party without the prior written consent from the RCMP;

4.6 limit access to the SIR to the SIR Users; and

4.7 comply with all physical, information technology, and personnel security requirements specified by the RCMP when handling protected and/or classified information.

The RCMP intends to:

4.8 treat all information received from the CI Stakeholder as confidential information;

4.9 take all reasonable measures to preserve the confidentiality and integrity of all information received from the CI Stakeholder against accidental or unauthorized access, use or disclosure.

5. PROTECTION OF INFORMATION

5.1 The RCMP will endeavour to protect all information received from the CI Stakeholder to the fullest extent permitted by law against disclosure due to, including without limitation, a request under the *Privacy Act*, the *Access to Information Act* or other lawful authority.

5.2 The information shared with the RCMP under this arrangement will be administered, maintained, and disposed of in accordance with the law that applies to record retention and personal information and all applicable policies and guidelines. This includes the *Privacy Act*, the *Library and Archives of Canada Act* and *Government Security Policy*;

5.3 The CI Stakeholder understands that information shared through the SIR may be subject to mandatory disclosure obligations resulting from a criminal prosecution or other legal obligation.

5.4 The CI Stakeholder will:

5.4.1 immediately notify the RCMP of any unauthorized use or disclosure of the information received under this MOU and will furnish the RCMP with the details of such unauthorized use or disclosure. The CI Stakeholder will also take all reasonably necessary steps to prevent any re-occurrence;

5.4.2 promptly notify the RCMP that it has received a lawful request for information received under this MOU. If requested, the CI Stakeholder will endeavour to protect the information from disclosure to the fullest extent permitted by law;

5.5 The RCMP will:

5.5.1 immediately notify the CI Stakeholder of any unauthorized use or disclosure of the information received under this MOU and will furnish the CI Stakeholder with the details of such unauthorized use or disclosure. The RCMP will also take all reasonably necessary steps to prevent any re-occurrence;

5.5.2 promptly notify the CI Stakeholder that it has received a lawful request for information received under this MOU. If the RCMP receives a request for the aforementioned information, the RCMP will endeavour to protect the information from disclosure to the fullest extent permitted by the law.

6. ACCURACY OF INFORMATION

The CI Stakeholder will:

6.1 use its best efforts to verify the accuracy of the information provided to the SIR;

6.2 promptly notify the RCMP if it learns that inaccurate or potentially unreliable information may have been provided or received from the SIR.

7. FINANCIAL ARRANGEMENTS

7.1 The CI Stakeholder will bear its own costs in carrying out its obligations under this MOU. For greater clarity, this includes the costs associated with maintaining secure office facilities, the acquisition of approved security containers, telecommunication equipment and software systems, among other things.

8. DEPARTMENTAL REPRESENTATIVES

The following officials are designated as the representatives for purposes of this Memorandum of Understanding and any notices required under this MOU will be delivered to:

For the RCMP: Name Title Address Telephone	For the CI Stakeholder: Name Title Address Telephone

Changes to the designated representative will be done by written notification to the other representative.

9. MONITORING

The RCMP will request on a yearly basis, and as required, input from all the Participants to assist in the review and assessment of the operation and effectiveness of this MOU.

10. LIABILITY & INDEMNITY

10.1 Each of the Participants will be responsible for any damages caused by the conduct of its employees, contractors or agents in carrying out the terms of this MOU.

10.2 The Participants acknowledge that other CI Stakeholders, police agencies, and federal departments/agencies having a signed MOU with the RCMP in relation to SIR access are each responsible for any damages caused by the conduct of their respective employees, contractors, or agents in carrying out the terms of their MOU.

11. DISPUTE RESOLUTION

In the event of a dispute arising from the interpretation of this MOU, the representatives will use their best efforts to resolve the matter amicably. If such negotiation fails, the matter will be referred to the signing authorities for resolution.

12. AMENDMENTS

No change or modification to this MOU is valid unless it is in writing and signed by the Participants.

13. TERM

This MOU commences upon ● and will terminate on ● unless terminated on an earlier date or otherwise extended by the mutual agreement of the Participants, in accordance with the terms of this MOU.

14. TERMINATION

14.1 This MOU may be terminated by the CI Stakeholder or the RCMP upon 30 days written notice.

14.2 Termination does not release the Participants from any obligations which accrued while the arrangement was in force and the obligations of confidentiality will survive the expiry or termination of this MOU.

SIGNING AUTHORITIES

Signed by the authorized officers:

For the CI Stakeholder:

_____ Date: _____

Name

Title

For the RCMP:

_____ Date: _____

Name

Title

Annex F Sample sOW - SCADA Risk Assessment Services

OBJECTIVE

The purpose of this Statement of Work (SOW) is to describe the work entailed in conducting a cyber-threat and risk assessment (CTRA) of the Supervisory Control and Data Acquisition (SCADA) components of [name of Critical Infrastructure Asset Owner]. [Provide a brief description of the facility/system in the body of the SOW; typically material from business project charters for the line of business responsible for the assets; all suitable plans, schematics and more detailed material are to be relegated to an annex.] As a minimum, the CTRA shall include:

- a Statement of Sensitivity (SOS) to identify and categorize relevant Critical Infrastructure (CI) assets according to their confidentiality, integrity and availability values based upon the injuries that may reasonably be expected in the event of a compromise;
- an identification of deliberate threats, accidents and natural hazards that might affect these assets adversely with an analysis of the likelihood of occurrence and gravity of impact;
- an assessment of current vulnerabilities, based on an evaluation of existing or proposed security measures and their adequacy;
- an analysis of residual risks for each asset which is vulnerable to specific threats; and
- where assessed residual risks exceed the [Low or Medium] level, a list of recommendations proposing additional safeguards to achieve a [Low or Medium] target risk level with an assessment of their effectiveness and cost.

TASKS AND DELIVERABLES

PREPARATION PHASE

GENERAL

Careful planning is required before initiating a CTRA to determine the scope of the assessment, identify resource requirements and develop a realistic work plan. To achieve these goals, the contractor must work in close cooperation with the Project Authority (PA), the Technical Subject Matter Experts (T-SMEs), security officials and facility or system managers. The contractor will be provided with all reference material, listed at

below, and any other information necessary for the completion of this task. Information-gathering activities may include interviews with personnel at various levels of the organization.

INITIAL PLANNING DELIVERABLES

The sole deliverable for the Preparation Phase is a complete CTRA Work Plan which includes:

- a clearly stated Aim for the CTRA;
- a statement of Scope with a description of the [facility or system] under consideration, its mission and concept of operation, as well as the boundaries of the assessment and any dependencies or interconnections with other [facilities or systems];
- any limitations or restrictions; [These may include intrusive penetration testing of production equipment, or other activities which may expose infrastructure to interference or compromise the health and safety of operators and other stakeholders.]
- the Target Risk Level accepted by the responsible manager;
- a list of personnel who will participate in the CTRA process as Team Members or sources of information; [Representation from affected business areas, operations managers, and technology subject matter experts (SME) is required.]
- all necessary Logistic Arrangements, including security screening and access requirements, travel arrangements, administrative support and other resource requirements;
- a list of Parties to the Assessment and their roles, Input Documentation and CTRA Deliverables; and
- a detailed CTRA Schedule listing all major activities, assigned resources, start and completion dates, and any dependencies.

THE THREAT AND RISK ASSESSMENT

GENERAL

Once the CTRA Work Plan has been approved at the end of the Preparation Phase, the contractor shall develop four mandatory deliverables to address the four-step CTRA process prescribed by this guide.

1. identify the employees and CI assets to be safeguarded in a Statement of Sensitivity;
2. determine the threats to employees and stakeholders and to CI assets and assessing the likelihood and impact of threat occurrence;

3. assess risk based on the adequacy of existing safeguards and vulnerabilities; and

4. recommend supplementary safeguards that will reduce the risk to an acceptable level.

CI ASSET IDENTIFICATION AND SENSITIVITY RATING PHASE

In the second phase, in a workshop with the key parties to the assessment, the contractor will facilitate the identification and listing of employees and stakeholders, CI assets and CI services within the scope of the assessment, and assign values for confidentiality, availability and integrity, based upon the perceived injuries that might reasonably be expected in the event of compromise. The results of this analysis in the workshop shall be approved by the parties who are authorized to accept risk on behalf of the CI Asset Owner, and the results shall be presented as a Statement of Sensitivity in a tabular form. This statement is the key deliverable for this portion of a CTRA project, and it must be annotated with the names of the parties who have accepted the assets and their sensitivities comprised by the scope of the assessment.

THREAT ASSESSMENT PHASE

The third phase of a CTRA project requires the contractor to identify imminent and potential threats that could reasonably be expected to adversely affect the health and safety of employees and stakeholders, CI assets, or CI services. Current information about threats should be obtained from security authorities [typically a qualification of the contractor] and the responsible lead agencies, specifically CSIS, CSEC and the RCMP. Key deliverables for this portion of the CTRA comprise:

- a tabular list of real and potential threats that could injure employees or compromise assets and services within the scope of the assessment; and

- an assessment of the likelihood and impact of their occurrence.

RISK ASSESSMENT PHASE

In the fourth phase of a CTRA project, the contractor will deliver an assessment of residual risks with regard to employees and stakeholders, CI assets and CI services. The two mandatory deliverables are the Vulnerability Assessment derived from an evaluation of existing or proposed safeguards and their effectiveness, and the Cyber Risk Assessment listing all residual risks to employees and stakeholders, CI assets and CI services within the scope of the assessment.

RECOMMENDATIONS PHASE

Based upon the findings of the risk assessment phase, the contractor will propose the addition, modification or removal of safeguards to achieve level of residual risk that is acceptable by the CI Asset Owner. The projected residual risk which remains after the recommendations have been approved and implemented shall also be identified with the recommendations. The CI Asset Owner may assess the perceived costs of the recommended changes and assess them against the residual risk from assessment.

PROJECT MANAGEMENT

PROJECT AUTHORITY (PA)

The PA for a CTRA must be an individual who has access to all parties of the assessment to ensure that requests for documentation and clarification are met, and that a quorum at the workshop is achieved as a foundation for the assessment.

The PA for this CTRA project is [name, position and telephone number of the overall coordinator of the CTRA project].

TECHNICAL SUBJECT MATTER EXPERTS (T-SMES)

The T-SMEs for this project are [names, positions and business e-mail addresses of designated subject matter experts who will provide technical input to the CTRA, including security authorities and facility managers; or programmers, engineers, millwrights and systems administrators, and other members of the CTRA Team].

CTRA METHODOLOGY

The contractor shall employ the Cyber Threat and Risk Assessment (TRA) Methodology for this project. It is intended to integrate with the existing Harmonized Threat and Risk Assessment (TRA) Methodology from CSEC. [Specify alternatives if applicable.]

PERSONNEL QUALIFICATIONS

The contractor shall provide personnel who have demonstrable experience and knowledge of:

the CTRA process; Critical Infrastructure Protection standards such as NERC CIP; and SCADA and other cyber/kinetic interfaces and control systems such as relays and programmable logic controllers (PLCs) in the scope of the assessment. Typically the experience is demonstrated by the successful completion of at least three previous Harmonized TRAs for critical infrastructure asset owners.

SCHEDULE

As stipulated above [if the contractor is to conduct the Initial Planning], the contractor shall develop a CTRA Work Plan with a detailed schedule showing milestones, critical activities and dependencies for the completion of the work by [a date specified by the contracting authority].

The contractor shall complete this CTRA project within [time frame cited in the CTRA Work Plan] following award of the contract, with intermediate deliverables submitted to the TA and PA in accordance with the approved CTRA Work Plan.

APPROVAL OF DELIVERABLES

All deliverables will be reviewed for quality and completeness, and signed off by the CI Asset Owner before proceeding to the next phase of the project. Where feasible, the PA should provide acknowledgement that that the CTRA methodology has been executed as a means to certify the integrity of the process on behalf of the assessment parties before the recommendations are delivered.

The CI Asset Owner should sign an acknowledgement that it has received the findings and recommendations, and this should be included with the acknowledgement of methodology execution.

PROGRESS REPORTING

This CTRA methodology recommends two key assessment checkpoints. The first is the methodology execution checkpoint, at which the contractor provides artifacts of the methodology to the project authority to show analytic completeness. The second is the presentation of the risk findings and recommendations to the project authority for acceptance by the CI Asset Owner.

The contractor shall provide periodic progress reports to the designated project authority. Verbal progress reports are acceptable. [Where written reports are preferable, specify the format and content].

PLACE OF WORK

In the interest of preserving the integrity of the CTRA process, all work shall be conducted at the contractor's place of business, except for interviews with departmental personnel which shall be coordinated with the designated TA. [If the CTRA project includes sensitive information, ensure that a facility security clearance with document safeguarding capability to the appropriate level has been specified above].

PROPRIETARY INFORMATION

All information and documents made available to the contractor during the course of this project are deemed proprietary to the CI Asset Owner, and shall be returned upon completion of the CTRA.

HANDOVER

The contractor shall table the following at a handover meeting arranged by the PA, within two (2) working days of the satisfactory completion of the project:

- a list of all changes to the deliverables in response to comments from the T-SME and PA;
- all final deliverables in [specify format and number of copies]; and
- all proprietary information and documents provided to the contractor during the project.

Annex G Cyber ics Asset Valuation Table

INSTRUCTIONS

1. Enter all assets within the scope of the CTRA project at the appropriate level of detail (Group, Subgroup and Component or Individual) from the Asset Listing.
2. Using the table below, based upon the maximum injury levels that could reasonably be expected to arise in the event of a compromise to their confidentiality (C), availability (A), integrity (I), and safety (S) insert the relevant asset values determined in accordance with the Injury Table below ranging from Very Low through High (VL through H).

Table 1: Graduated Injury Table			
Level of Injury	**Injury to People**		**Financial Impact**
	Physical	**Psychological**	
Very High	Widespread Loss of Life	Widespread Trauma	> $100 million
High	Potential Loss of Life	Serious Stress/Trauma	> $10 million
Medium	Injury/Illness	Public Suspicion/Doubts	> $100 thousand
Low	Discomfort	Minor Embarrassment	> $1 thousand
Very Low	Negligible	Negligible	< $1 thousand

Annex H Cyber Control Systems Asset Listing

The following table is a taxonomy of asset types for CI Asset Owners and the types of SCADA system related assets that will be assessed in the course of the CTRA. Critical Infrastructure comprises people, processes and technology, and the following table is intended to assist in grouping the assets under assessment for completeness and as a guide to determine CTRA scope. Use these example assets as a guide for developing an accurate asset list for the scope CTRA. In developing the list, consider whether a compromise of the Availability, Integrity or Confidentiality of the asset might have a business or safety impact on the CI Asset Owner, or on employees and stakeholders, CI assets and CI services.
This Asset Listing is included as an example and is not considered to be complete.

Class	Category	Group	Subgroup	Individual Asset
PLC				
			Programmable Logic Controllers	
			Relays	
			Sensors	
			Indicators and Signals	
			Development and Debugging interfaces	
			Interfaces to SCADA systems	
SCADA				
	Management			
		HMI	Software	
		Interfaces	Operating systems	
			Software packages	
			Development Frameworks and Environments	
			Application Platforms	
			Networks	
			Embedded devices	

Class	Category	Group	Subgroup	Individual Asset
			Embedded operating systems	
		SCADA System Data	Sensor Information	
			Telemetry Data	
			Liquid and Gas Flow	
			Valve Operation	
			Radar Images	
			Power Usage	
			Capacity	
			Current	
			Geolocation Data	
			Hydraulics Operation	
			Cryptographic Data	
		Physical Interfaces	USB/Serial/Parallel Interfaces	
			IR Interfaces	
			Network Interfaces	
			Inputs	
			Antenna ports/RF Interfaces	
			Board/Chip Debugging Interfaces	
	Network Infrastructure Components	Routers		
		Hubs		
		WiMAX nodes		
		WiFi nodes		

Class	Category	Group	Subgroup	Individual Asset
		3G/4G Networks		
		Cellular networks		
		900 MHz Wireless Routers		
		Satellite Connections		
		VPN Termination		
		Power Distribution Automation		
		Telephone Poles		
		Radio Communications		
		Microwave	Repeaters	
		Rail fibre optic cable paths		
		Public RF Band Comms.		
		Spread Spectrum Comms.		
		Mesh Communications		
		Network Policy Devices	Firewalls	
			IDS/IPS	
			IAAA Services and Interceptors	
			AV	
		Security Components	Cryptographic Devices	
			Biometric Equipment	
			IAAA Tokens	Passwords, keys, certificates

Class	Category	Group	Subgroup	Individual Asset
			Advanced Card Technologies	
			Secure Remote Access Devices	
		Media	Tapes	
			Diskettes	
			CDs	
			DVDs	
			CD ROM	
			USB Drives	
			Hard Drives	
		Firmware	Embedded Operating Systems	
				uCLinux
				WinCE
				PicoBSD
				OpenBSD
				CentOS
				Android
				Java
				Assembly
				Ladder Logic
		Development Environments		
			Embedded software development	
			Ladder Logic development	
			Staging environments	
		Hazardous	Combustible Liquids	

Class	Category	Group	Subgroup	Individual Asset
		Materials		
			Compressed Gases	
			Corrosive Chemicals	
			Flammable Aerosols	
			Flammable Gases	
			Flammable Liquids	
			Flammable Reactive Agents	
			Flammable Solids	
			Oxidizing Agents	
			Reactive Agents	
		Kinetic Systems		
			Rotors	
			Engines	
			Valves	
			Hydraulics	
			Fans	
			Wheels	
			Gears	
			Levers	
			Robotics	
			Elements and Heat Sources	
			Spark plugs	
			Lasers	
			Cutters	
			Clamps	
			Elevators	
			Turbines	

Class	Category	Group	Subgroup	Individual Asset
			Conveyers	
Power				
	Distribution & Automation			
		Network	Radios	
			Cellular comms	
			Repeaters	
			Capacitance measurement	
			Monitoring Equipment	
			Transformers	
			Substation	
			CO	
			Mesh nodes	
		Smart Grid	Cryptographic keys	
			Smart Meter Infrastructure	
			Meters	
			Relays	
			Last mile wireless	
			Mesh networks	
	Generation			
		Nuclear	Centrifuges	
			Coolant Systems	
			Reactor systems	
			CANDU components	
			Fuel Management	

Class	Category	Group	Subgroup	Individual Asset
			Heavy water management	
			Component threshold monitors	
			Waste management	
		Hydro Electric		
			Dam	
			Locks	
			Valves	
			Hydraulics	
		Solar		
			Smart Grid Infrastructure Demarcation	
			Batteries	
		Wind	Turbine controls	
			Batteries	
			Monitoring	
			Smart Grid Infrastructure Demarcation	
		Coal		
			Furnace	
			Fuel management	
			Coolant management	
			Waste Water Management	
			Environmental Controls	
			Waste Water Management	
			Environmental Controls	
			Temperature monitoring	

Class	Category	Group	Subgroup	Individual Asset
Transportation				
	Rail		Signalling Systems	
			Relays	
			Switching systems	
			Route management	
			GPS	
			Speed management	
			Engine control	
			Streetcar/Trolley management	
			Subway management	
			LRT management	
			Safety management	
			Container monitoring and controls	
			Crossing controls	
	Highway and Traffic Mgmt.			
			Traffic lights and signals	
			Automated Signs	
			Mobile Signs	
			Bridge controls	
			Gate control	
			Speed measurement	
			"Red light" cameras	
			Toll systems	
			Emergency services override	
	Fleet Mgmt.			
			Location beacons	

Class	Category	Group	Subgroup	Individual Asset
			Operator communications	
			Freight load data	
			Speed data	
	Air Traffic			
			Radar	
			"Fly by wire" Systems	
			Aircraft Identification	
			Landing Lamps and Beacons	
			Air Traffic Management Displays	
			Controller/Pilot communications	
			Airport Perimeter Security	
			Cargo handling/treadmills	
			Boarding Gate Hydraulics	
			Scheduling and Routing	
			Airport Information Displays	
			Signalling Systems	
Pipelines			Waste water	
			Water filtration	
			Hydraulics	
			Contaminant management	
			Chemical treatment	
			Pressure	
			Flow	
			Oil	
			Valve Operation	
Defense			Radar/Sonar	
			Fleet management	
			Location Services	

Class	Category	Group	Subgroup	Individual Asset
			Aerial Drones	
			Guidance systems	
			Mesh comms.	
			Satellite comms.	
			Shipboard management.	
			Cryptographic materials	
			FOF systems	
			Bomb disposal robots	
Law Enforcement				
	Command and Control		Emergency Services Dispatch	
			Fleet Management	
			Location based services (GPS)	
			Radio Communications	
			Radio Mesh Comms	
			Data Mesh Comms.	
			Emergency services override	
			Pager/text data comms.	
			GPS and locative data	
	Surveillance		GPS	
			Vehicle tracking	
			Personnel tracking	
			Camera and optical sensor controls	
			Interception equipment	
			Video signals	

Class	Category	Group	Subgroup	Individual Asset
	Automation		Bomb disposal robots	
			Aerial drones	
			Facilities management	
			HVAC	
			Door and gate access	
			Immobilizers	
			Correctional Facility Controls	
			Print and Copy services	

Annex I Threat Listing

Instructions: Select Classes and Activities for the evaluation and use the example Agents and Events to construct scenarios in which the assets of the organization are exposed to the threat. Regardless of how exotic the threat may seem, their impact on the assets will tend to affect the confidentiality, integrity, availability or safety of the asset. It is useful to focus on the occurrence of the event, independent of whether participants perceive it as likely, since it is a means to determine the full impact and in turn, whether the threat should be included in the evaluation.

SCADA assets in remote locations are in particular sensitive to natural hazards and the lack of availability of staff to monitor or repair them, and when considering threats to the availability of assets, contingencies for natural hazards should be taken into account.

	Class	Activity	Agent Category	Agent	Event
1.	Deliberate	War	Nation States	Military and Paramilitary	
2.					Information Operations
3.					Infrastructure Attack/Sabotage
4.					Attack Deterrent
5.					Third Party Intervention Deterrent
6.					Development of Deterrent Capability
7.					Attack Alliance Member
8.					Demonstrate Cyber-warfare Capability
9.					Delay/Destroy Planned Infrastructure Project
10.		Civil Conflict	Faction	Hackers	Infrastructure Seizure/Resource Control
11.					Demonstrate Cyber-warfare Capability
12.					Terrorism
13.					Sabotage
14.					
15.					
16.		Espionage	Foreign Intelligence Service	Services	COMINT
17.					ELINT

	Class	Activity	Agent Category	Agent	Event
18					Emanations Interception
19.					Network Exploitation
20					HUMINT
21.					IMINT
					Infiltration
22.					Open Source Collection
23.					Break and Enter
24.			Other State Sponsored	Organizations	Repeat Serials 1-10.
25.			News Media	Companies	
26.					Demonstrate Vulnerability
27.					
28.					
29.			Industrial Espionage	Companies/States	
30.					Electronic Eavesdropping
31.		`			Reverse Engineering
24.					Competitive Intelligence
25.					Break and Enter
29.			Hackers	Groups	Network Exploitation
30.					Reverse Engineering
31.				Individuals	Network Exploitation
32.					Reverse Engineering
33.			Organized Crime	Groups	HUMINT
34.					Electronic Eavesdropping
35.					Network Exploitation
					Market Manipulation (equities, commodities, options)
					Extortion
36.		Sabotage		Organizations	Information Operations

	Class	Activity	Agent Category	Agent	Event
			Vendor	OEM	Undocumented “tech support” access.
				Outsourced Software Developer	Hidden backdoor in source code
				Systems Integrator	Undocumented “tech support” access.
				Manufacturer	Undocumented functionality
					Backdoor access
					Compromises Cryptographic Implementation
					Compromised Security Controls
37.			Competitor	Organizations	Product Tampering
					Market Manipulation
38.			Disgruntled Employees	Groups/Individuals	
39.					Vandalism
40.					Delete/Destroy Records
41.					Corrupt Data
42.					Encrypt Files
43.					Misconfigure Software
44.					Misconfigure Hardware
					Backdoor Access
					Bargaining Position
					Extortion
45.			Activists	Radical Groups	
					Destroy Equipment
					Demonstrate Vulnerability
					Degrade Service

	Class	Activity	Agent Category	Agent	Event
46.			Hackers	Casual	Denial of Service Attacks
47.					Command Execution
48.					Intelligence Gathering
49.					Repeat Serials 46-48.
50.					Repeat Serials 46-48.
51.					Repeat Serials 46-48.
				Automata	Botnets
					Worms
					Advanced Persistent Threats
					Viruses
				Targeted Attacks	
				Academic Proof of Concept Attacks	
				Advanced Persistent Threats	
				Technological Breakthrough	New exploits, broken cryptosystem, “0-day”, etc.
52.		Subversion			
53.			Political Activists	Groups	Demonstrate Cyber-warfare Capability
54.					Delay/Destroy Planned Infrastructure Project
55.					Demonstrate Cyber-warfare Capability
56.					
57.			Competitors	Organizations	Rumours to damage user confidence in infrastructure or service.
58.					(False) Advertising
59.			Labour Unrest	Groups	Sabotage
60.			Hackers	Script Kiddies	Web Defacement
61.					Hoaxes
62.				Fully Capable	Repeat Serials 60-61.
63.				Elite Hackers	Repeat Serials 60-61.
77.		Criminal Acts	Insiders	Employee(s)	
78.					Sabotage

	Class	Activity	Agent Category	Agent	Event
79.					Data Interception
80.					Market Manipulation (equities, commodities, options)
81.					Fraud
84.					Property Damage
85.					Extortion
86.				Temporary Help	Repeat Serials 77-85.
87.				Subcontractors	Repeat Serials 77-85.
88.				Service Staff	Repeat Serials 77-85.
89.				Security Guards	Repeat Serials 77-85.
90.			Outsiders	Clients	Repeat Serials 77-85.
91.				Contractors	Repeat Serials 77-85.
92.				Visitors	Repeat Serials 77-85.
93.				Public	Repeat Serials 77-85.
94.				Hackers	Identity Theft
95.					
96.				Petty Criminals	
97.					Theft of SIM cards
98.					Theft of Service
99.			Organized Crime	Groups	
100.					Theft of SIM cards
101.					Theft of Service
102.					
110.			Organized Labour/Unions	Groups	Work to Rule
111.					Work Slowdowns
112.					Work Stoppages
113.					Block/Delay Access
114.			Demonstrators	Activist Groups	Peaceful Marches
115.					Blocking Roadways
116.					Violent Confrontations
117.					Riots

	Class	Activity	Agent Category	Agent	Event
118.					Building Occupations
119.				Political Independence and Pressure Groups	Repeat Serials 114-118.
120.				Organized Labour	Repeat Serials 114-118.
121.	Accidents	Office Accidents	Employees	Office Staff	Delete Files
125.					Forget Password
127.		Lost Assets	Employees	Individuals	Lost Notebook Computers
128.			Contractors	Organization	Misdirect Shipments
129.		Data Corruption	Employees	Data Entry Clerks	Data Entry Errors
130.				Data Base Admin.	Operating Errors
118.			Clients	Individuals	Inaccurate Data Input
131.		Software Errors	Software Vendors	Companies	Software Bugs
132.			System Integrators	Organizations	Software Integration Errors
133.			Internal Programmers	Individuals	Coding Errors
134.			System Administrators	Individuals	Software Configuration Errors
135.		Hardware Failures	Hardware Vendors	Companies	Design Flaws
136.					Equipment Malfunction
137.			System Integrators	Organizations	Installation Errors
138.			System Administrators	Individuals	Hardware Configuration Errors
139.					Operator Errors/Misuse
140.		Mechanical Failures	Equipment Vendors	Companies	Design Flaws
141.					Equipment Malfunction
142.			Public Utilities	Organizations	Water Outage
143.					Power Failures
144.			Building	HVAC Maintainers	Loss of Heating

	Class	Activity	Agent Category	Agent	Event
			Custodians		
145.					Condensation
146.				Plumbers	Leaks/Water Damage
147.			Equipment Operators	Individuals	Inadvertent Misuse
148.		Structural Failures	Architects	Companies	Design Flaws
149.			Construction Industry	Companies	Substandard Construction
150.			Building Occupants	Organizations	Overstress Floors
154.		Industrial Accidents	Transportation Workers	Truck Drivers	Toxic Spill
155.			Manufacturing Teams	Equipment Operators	Personal Injury
156.					Disrupt Production
157.		Traffic Accidents	Employees	Individuals	Private Motor Vehicle Accident
158.				Transport Drivers	Public Motor Vehicle Accident
159.		Nuclear Accidents	Nuclear Power Plant	Operations Staff	Radiation Leak
160.					Core Melt Down
161.			Medical Facilities	Medical Staff	Accidental Overdose
179.		Earth Movement	Erosion	Water Erosion	Undermine Building
180.				Wind Erosion	Strip Topsoil
181.			Land Subsidence	Groundwater Loss	Undermine Building
182.					Roadway Sinks
183.					Local Flooding
184.				Carbonate Rock	Repeat Serials 181-183.
185.			Landslides	Rainfall/Seepage	Buildings Collapse

	Class	Activity	Agent Category	Agent	Event
186.					Disrupt Transportation
187.				Water Erosion	Repeat Serials 185-186.
188.			Volcanoes	Lava Flows	Destroy Buildings
189.					Disrupt Movements
190.					Block Water Flows
191.				Volcanic Ash	Bury Buildings
192.					Suffocate People
193.					Contaminate Water Supplies
194.			Earthquakes	Interplate Earthquake	Micro (2.0 Richter Scale)
195.					Minor (2.0-3.9)
196.					Light (4.0-4.9)
197.					Moderate (5.0-5.9)
198.					Strong (6.0-6.9)
199.					Major (7.0-7.9)
200.					Great (8.0-8.9)
201.					Rare Great (9.0-9.9)
202.				Intraplate Earthquake	Repeat Serials 194-201.
203.		Flooding	Lake	Specific Site	Spring Runoff
204.					Ice Dam
205.					Flash Flood
206.			River	Specific Site	Repeat Serials 203-205.
207.			Ocean	Specific Site	High Tide
208.		Environmental	Airborne Particles	Dust	Media Contamination
209.				Pollen	Allergic Reactions
210.			Temperature	Heat Wave	Dehydration/Death
211.				Extreme Cold	Frostbite
212.				Prolonged Cold	Loss of Life
213.			Humidity	High Humidity	Dry Rot/Structural Damage
214.					Spores/Allergic Reactions
215.				Low Humidity	Static Electricity
216.			Magnetism	Geomagnetism	Navigational Interference
217.			Radiation	Radon Gas	Health Hazard
218.			Static Electricity	Static Discharge	File Corruption

	Class	Activity	Agent Category	Agent	Event
219.			Stellar Phenomena	Cosmic Rays	Cell Damage
220.				Meteors	Damage Satellite
221.				Sunlight	Acute Sunburn
222.					Damage Exposed Fabric
223.				Geomagnetic Storms	Disrupt Communications
224.					Power Outage
225.		Severe Storms	High Winds	Hurricanes	Category 1 Saffir-Simpson
226.					Category 2 Saffir-Simpson
227.					Category 3 Saffir-Simpson
228.					Category 4 Saffir-Simpson
229.					Category 5 Saffir-Simpson
230.				Tornadoes	F0 Fujita Scale
231.					F1 Fujita Scale
232.					F2 Fujita Scale
233.					F3 Fujita Scale
234.					F4 Fujita Scale
235.					F5 Fujita Scale
236.					F6 Fujita Scale
237.				Typhoons	Repeat Lines 225-229.
238.			Thunderstorms	Lightning Strikes	Power Surge
239.					Power Outages
240.					Fire
241.				Severe Rainfall	Flooding
242.			Snowstorms	Heavy Snowfall	Traffic Congestion/Delays
243.					Power Outages
244.			Hailstorms	Large Hailstones	Crop Damage
245.			Freezing Rain	Ice Accumulation	Falling/Personal Injuries
246.					Vehicle Accidents
247.					Power Outages

This Threat Listing is not intended to be complete. It is a reference for the types of threats faced by operators of critical infrastructure and SCADA solutions.

Annex J Threat Assessment Table

INSTRUCTIONS

Enter all CIP threats within the scope of the CTRA project at the appropriate level of detail (Threat Activity, Threat Agent Category, Threat Agent and Threat Event) based upon the contents of the supplied Cyber Threat Listing and in conjunction with site specific threats which might not be captured in the materials template.

Based on the statement of sensitivity, and expert threat intelligence, determine the relevant levels for each threat ranging from Very Low through High (VL through H) with respect to the confidentiality (C), availability (A) and/or integrity (I) and Safety (S) of the affected assets.

Focus on the Impact of the threat event, and less on the likelihood (or perceived probability), since many threats are discounted as "impossible", or "could never happen" before they occur.

EXAMPLES

SABOTAGE

If the Sabotage threat posed by foreign military were assessed to be High with respect to the (I)ntegrity and (A)vailability of smart grid control systems, based upon the likelihood of occurrence and the perceived capabilities of the adversary, but the confidentiality of the assets were lower, and there was no significant consequences for human safety or quality of life, the threat would be expressed using the following Threat Assessment Table:

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels				Asset(s)
					C	A	I	S	
Deliberate	War	Nation State	Military and Paramilitary	Demonstrate Cyber-warfare Capability	M	H	H	M	SCADA System Data; Network Components; Embedded Operating Systems

HACKER

If a hacker motivated by organized criminal's intent on market manipulation obtained unauthorized access to SCADA system data from oil refinery operations, the (C)onfidentiality threat would be considered High. It would also be considered High for (A)vailability due to the opportunity and means to commit denial of service attacks against the refinery communications infrastructure, impacting production. Unauthorized modification of the data (Integrity) is less probable due to both implied safeguards, and the balance of effort vs. incentives. The (S)afety impact is minor since data is being intercepted and not transmitted or altered.. This would be expressed by the following entries in the Threat Assessment Table:

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels				Asset Subgroup(s) Affected
					C	A	I	S	
Deliberate	Espionage	Organized Crime	Hackers	Market Manipulation (equities, commodities, options)	H	H	L	L	SCADA System Data: Liquid and Gas flow
Deliberate	Sabotage	Vendor	OEM	Undocumented "tech support" access.	M	H	M	M	Network Infrastructure Components: Mesh Network Routers

SOFTWARE ERROR

A software error is discovered and published on the Internet and the vendor releases a patch which must be applied to the system to maintain warranties and service level agreements. The software is used to manage a real-time pipeline control system that runs 24/7/365 and is not designed to be taken out of service for maintenance without interrupting the flow of gas to major distribution centres. The (C)onfidentiality threat would be Very Low (or NA), (A)vailability threat would be High, the (I)ntegrity threat would be Medium and the (S)afety threat would be Low.

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels	Asset(s) Affected

					C	A	I	S	
Accidental	Software Error	-	Software Vendor	Coding Error	VL	H	M	L	Embedded Devices; Liquid and Gas flow; Valves;

The choice of assets in the scope of the assessment will determine the types of threats included in the analysis. These tables are intended to track threats to assets for inclusion in the risk assessment. The assets should reflect the elements of the business and the infrastructure and the threats should reflect the operational realities of the day and of the foreseeable future.

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels				Asset(s) Affected
					C	A	I	S	
Deliberate	Espionage								
	Sabotage								
	Subversion								
	Terrorism								
	Criminal Acts								
	Others								
Accidental	Office Accidents								
	Data Corruption								
	Software Errors								
	Hardware Failures								
	Mechanical Failures								
	Structural Failures								
	Fires								
	Industrial Accidents								
	Nuclear Accidents								

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels				Asset(s) Affected
					C	A	I	S	
Legend C – Confidentiality. A – Availability. I – Integrity. S – Safety.									

Annex K Vulnerability and Risk Sources

Vulnerability Class	Vulnerability Group	Risk Source	Impact		Affects		
			Likelihood	Impact	C	A	I
Security Program	Roles and Responsibilities	Executive sponsorship					
		Program Managers accountability					
		Project Managers responsibility					
		Chief Information Officer engagement					
		Employees awareness					
		IT Security Coordinator					
		BCP Coordinator					
	Security Policy/Procedures	Sharing Information/Assets					
		Contracting					
		Security Awareness/Training					
		Identification of Assets					
		Security Risk Management					
		Access Limitations					
		Security Screening					
		Protection of Employees					
		Physical Security					
		IT Security					
		Security in Emergencies					
		Business Continuity Planning					
		Security Program Audit					
		Investigation of Incidents					
		Sanctions					
Sharing Information/Assets	Information	Arrangements					
	Facilities	Arrangements					
	IT Infrastructure	Arrangements					
Security Outside Canada	Special Standards	TRAs by Location					
	Travel Restrictions	By Location					

Vulnerability Class	Vulnerability Group	Risk Source	Impact		Affects		
			Likelihood	Impact	C	A	I
Contracting	Roles and Responsibilities	Project/Technical Authority					
	Facility Security Clearance	Personnel Assigned					
		Document Safeguarding					
	International Contracts						
Security Awareness/Training	Roles and Responsibilities	Training/Awareness Officer					
	Security Training						
	Security Awareness	Initial Briefings					
		Regular Updates					
Identification of Assets	Confidentiality	Categorization: Classified					
		Marking: Classified					
		Categorization: Protected					
		Marking: Protected					
	Availability	Categorization					
		Marking					
	Integrity	Categorization					
		Marking					
Security Risk Management	TRAs	Initial Assessment					
		Continuous Monitoring					
Access Limitations	Classified/Protected Assets	Need to Know					
		Security Screening					
	Availability/Integrity	Separation of Duties					
Security Screening	Reliability Status	Establishing Requirements					
		Initial Screening					
		Evaluating Results					
		Regular Updating					
		Review for Cause					
		Revocation					
		Release Procedures					
	Security Clearance	Establishing Requirements					

Vulnerability Class	Vulnerability Group	Risk Source	Impact		Affects		
			Likelihood	Impact	C	A	I
		Initial Screening					
		Evaluating Results					
		Regular Updating					
		Review for Cause					
		Revocation/Downgrading					
		Release Procedures					
	Site Access Clearance	Establishing Requirements					
		Initial Screening					
		Evaluating Results					
		Regular Updating					
		Review for Cause					
		Revocation					
		Release Procedures					
Protection of Employees	Identify Employees at Risk	TRA					
	Management Response	Protective Measures					
		Support Mechanisms					
		Training and Counselling					
	Incident Management	Incident Reporting					
		Incident Investigation					
		Remedial Action					
IT Security	Management Controls	System Development Life Cycle					
		IT Security Resources for Projects					
		Certification and Accreditation					
		Contracting					
		Outsourcing					
	Technical Safeguards	Evaluated Products					
		Code Validation and Security Review					
		Identification and Authentication					
		Authorization/Access Control					
		Cryptography					
		Public Key Infrastructure (PKI)					

Vulnerability Class	Vulnerability Group	Risk Source	Impact		Affects		
			Likelihood	Impact	C	A	I
		Perimeter Defence					
		Mobile Computing/Telework					
		Wireless Devices					
		Emanations Security					
		Telecommunications Cabling					
		Software Integrity					
		Software Security Configuration					
		Malicious Code Protection					
		Intrusion Detection					
		Backup/Recovery					
	Operational Safeguards	Help Desk/Problem Resolution					
		Incident Management					
		Vulnerability Assessments					
		Patch Management					
		IT Continuity Planning					
		IT Security Assessment/Audit					
		Configuration Management					
		Change Control					
		Capacity Planning					
		Hardware Maintenance					
		Environmental Protection					
		Power Conditioning/Backup					
SCADA	Technical Vulnerability	HTTP Server Side Vulnerabilities					
		SQL Command Injection					
		Unpatched Software or OS					
		Unmaintained Proprietary OS					
		HTTP Client Side vulnerabilities					
		Default Login Credentials					
		Buffer Overflows					
		Race Conditions					
		Format String Errors					
		Undocumented Interfaces					

Vulnerability Class	Vulnerability Group	Risk Source	Impact		Affects		
			Likelihood	Impact	C	A	I
		Web Application Framework Vulnerabilities					
		Cryptologic Implementation Errors					
		Lack of Audit Trail					
		Privilege Escalation					
		Broad Privileges					
Business Continuity Planning	Governance Structure	Authorities					
		Responsibilities					
	Business Impact Analysis						
	Plans/Arrangements						
	BCP Program Readiness						
	Review, Testing and Audit						
Investigation of Incidents	Incident Investigation						
	Incident Reporting						
Sanctions	Security Violations						
	Security Breaches						

Notes:

The primary effect(s) of vulnerabilities related to inadequacies associated with any given safeguard are indicated in the foregoing table under Impact.

3 Introduction – Task 3- Define the Scope and Capabilities of a Cyber-Threat and Vulnerability Management System

This section reports on specific tasking as it pertains to 'Define the Scope and Capabilities of a Cyber-Threat and Vulnerability Management System'. The tasking in this project area was comprised of several activities, all of which assisted in developing aspects of a future-state cyber-situational awareness capability (bearing in mind that it may feed into a national cyber-situational awareness capability).The tasking was performed to align with proposed activities, and included:
Assess existing and proven management system frameworks and define requirements through collected stakeholder input

Design specifications using (where possible) existing technology

Assess alignment with any known Situational Awareness functions

During the study, it was not possible to ascertain the definitive characteristics of any such management system as it exists is in Canada, however the information collected from stakeholder collaboration efforts and other national capabilities resulted in some good results. In absence of any obvious national-level capability for SCADA, as well as not having access to the government representation able to accurately define current or planned threat and vulnerability management systems, the study team expanded their review of existing private/public sector sharing initiatives (focused on SCADA). The study team correlated findings from existing situational awareness capabilities (non-Canadian) and extracted common themes that could be used to support a cyber-threat/management system for Canadian critical industrial control systems assets and activities.

The study team selected common activities associated with 'focused national actions', and developed a framework to allow stakeholders to contribute to which information feeds and sharing forums would support such a capability. The study showed that effective threat and vulnerability management systems are not dedicated solely to understanding the threats and vulnerabilities themselves, but rather they support how information can be used to provide for a proactive (protection) and reactive (recovery) lifecycle. In addition, the study showed that the best approach for a SCADA cyber threat and vulnerability management system incorporates features and characteristics of past management frameworks, and that certain aspects of traditional management frameworks can work well in future-state strategies.

Using an approach that would ensure alignment with Canadian interests (should one exist or evolve over time) the study showed that the core areas of Operations, Watch and Warning, Analysis, Planning, Assist/Assess and Outreach provide an excellent set of domains for a SCADA cyber-threat and vulnerability management system. Perhaps more importantly, interaction with project partners and asset owners showed that these elements would (a) support effective information exchange between government and private sector, (b) help encourage private sector enrolment, and (c) create a management system that would dovetail into supporting cooperative incident response functions.

This document is intended to provide content to be used in the material to be delivered in the Final Project Study Report.

Section 2 is dedicated to discussing tasking activities, and provides insight to process, procedures, and investigative models used during the tasking. Section 3 discusses the findings and observations from the study activities, and presents the framework derived from study activities. Section 4 discusses conclusions, followed by an Appendix that provides overall project workflow.

3.1 Description of tasking activities

The primary task element, as a function of the overall study methodology, is shown in figure 1 below. This is derived from the Study Workflow as shown in Appendix A.

Figure 1 - Detailed workflow for Task 3

Lofty Perch and project partners have developed and/or supported cyber-threat and vulnerability management systems in both public and private sector. Through relationships with partners, the team established the SCADA Situational Awareness Group (SSAG) to determine a baseline set of requirements a management system would require. Unfortunately, due to scheduling issues, the SSAG was only able to help establish an initial the set of framework elements and not remain as a cohesive group during tasking. The study team mitigated this issue by enrolling input and support from other project partners on an as-needed basis, and used specific areas of expertise to define some of the more granular aspects of the management system's capability. Ultimately, this approach provided a set of requirements that could be interpreted to establish a SCADA threat and vulnerability management systems.

As information sharing was determined to be a critical part of the systems success, the study team revisited the existing frameworks for public/private information sharing. Using findings from previous project study activities, it was determined that existing information sharing frameworks are adequate to facilitate public/private sharing. The study did address high-level activities that government could implement to support the management system. The study team was able to leverage their experience in supporting similar programs around the world, and looked specifically at those projects involving the management of national cyber situational awareness activities as they pertain to SCADA.

One of the more interesting challenges of the tasking was determining what the technology landscape for such a management system would look like. To address this issue, the study team interacted with private and public sector partners that had either fully developed or were it the process of developing a vulnerability/threat management system that could accommodate SCADA datasets. The study shows that a common approach was to use 'activity' states to define what the management system is doing and how it supports proactive (steady state) or reactive (response) actions. This, in turn, helped the study team review a set of applicable operational components and the corresponding partners that would be required to ensure the management system remains effective.

3.2 Findings and observations

Using a number of different frameworks, the study team found that the approach that blends traditional and next-generation threat/vulnerability management systems together is a viable approach. The study activity focused on the system attributes deemed most useful by the Canadian stakeholder community. By assessing what has worked elsewhere, the study showed that there are several common attributes in systems designed to manage cyber threat and vulnerability information. Moreover, the collaboration with project stakeholders identified a set of characteristics that are not only desirable for a national capability but already exist at the asset owner level. Overall, the elements identified that would prove vital to a SCADA-specific threat and vulnerability management system are Operations, Watch and Warning, Analysis, Planning, Assist and Assess, and Outreach.

Operations: This function supports the coordination of interagency operational SCADA incident management efforts from the centres that are dedicated to cyber security, network security, sector-specific operational capabilities and other entities that focus on proactive and reactive security efforts

Watch and Warning (WW): Often defined within a primary centre for data aggregation, this capability fuses information from the Operations group/groups (above) with other SCADA open-source and sensitive outside information. Many management systems often allow this function to provide situational awareness or a 'Common Operating Picture (COP)' and can disseminate reports based on collected and analyzed intelligence.

Analysis: The Analysis function can provide support to the threat/vulnerability management system either prior to aggregation in the WW environment or it can assesses products from the WW and provided analysis for future SCADA trending. The Analysis group traditionally works closely with partners and stakeholders to generate information products for users in the intelligence community and asset owner domains, and a system focused on SCADA and controls systems could use the approach as well.

Planning: Supporting the Operations group, Planning facilitates how the management system handles the collection and dissemination of SCADA security information into the primary threat/vulnerability effort. This Planning group defines how information is disseminated based on intra-group coordination and maintains a focus on policy as it pertains to the collection of threat and vulnerability data. The Planning function also provides for developing the procedures for outreach

Assist and Assess: This function supports any technical assistance required onsite, should the requestor be part of the information sharing community or a SCADA asset owner. Usually not inclusive of criminal investigations, the Assist and Assess function provides proactive and reactive services that can include incident response, training, security assessments, and general security support for SCADA system owners.

Outreach: Often perceived as the most important function of any threat and vulnerability management system, this Outreach function provides support and assistance to those stakeholders and asset owners that depend on information sharing for day-to-day security operations. The study showed that this capability is vital to ensuring there is a point of contact for assisting and coordinating activities between agencies and CIP stakeholders, particularly with regard to IC and law enforcement relationships with SCADA system operators and infrastructure asset owners.

The study showed that requirements for a SCADA Threat and Vulnerability Management system must be viewed in the context of existing vulnerability management solutions. This was confirmed by project members and partners, and highlighted the approach to re-use process and technology to accommodate for the nuances associated with cyber security in the industrial automation domain. State of the art technical Vulnerability Management Solutions (VMS) are designed around the principle of continuous, differential vulnerability scanning and assessment, and this characteristic is required to ensure future-state approaches are sound. Information from different domains is aggregated from 'edges' to a central analysis function, which reports changes in the vulnerability environment to operators.

3.3 First Generation Vulnerability Management: "Find and Fix"

These solutions have evolved from the first generation of vulnerability management, which was a manual process, illustrated in the pattern diagram below. A security analyst, typically a systems administrator would seek out vulnerability information on the Internet via online forums, mailing lists, and chat rooms, then distribute it to functional areas for remediation. Vulnerability information was not "managed" so much as it was responded to by the people best able to deal with "fixing" the problem. The information was rarely disclosed beyond system departments, except in the rare case of a security incident that required the involvement of business decision makers or law enforcement.

Sources of vulnerability information were both formal and informal, beginning with new vulnerability information being shared among hackers, to leaking it to internet mailing lists and, at the time, newsgroups. Organizations like CERT, FIRST, COAST, and later, CANCERT and OCIPEP, began to collect and distribute the information in the public sector, where much of it originated from one or two websites in the private sector. While the threat to SCADA systems was widely known, the development of security practices largely related to internet vulnerability, where most SCADA systems were at the time connected by dial-up, leased lines, x.25 and proprietary networking technologies. The current state of SCADA networks (in 2011) still resembles this "Find and Fix" pattern to a great extent, since many Internet security systems have evolved separately from SCADA network security systems. The study showed that, as expected, SCADA expertise remains in the domain of specialized technical subject matter experts who are often the most well equipped to remediate individual vulnerabilities as they are discovered.

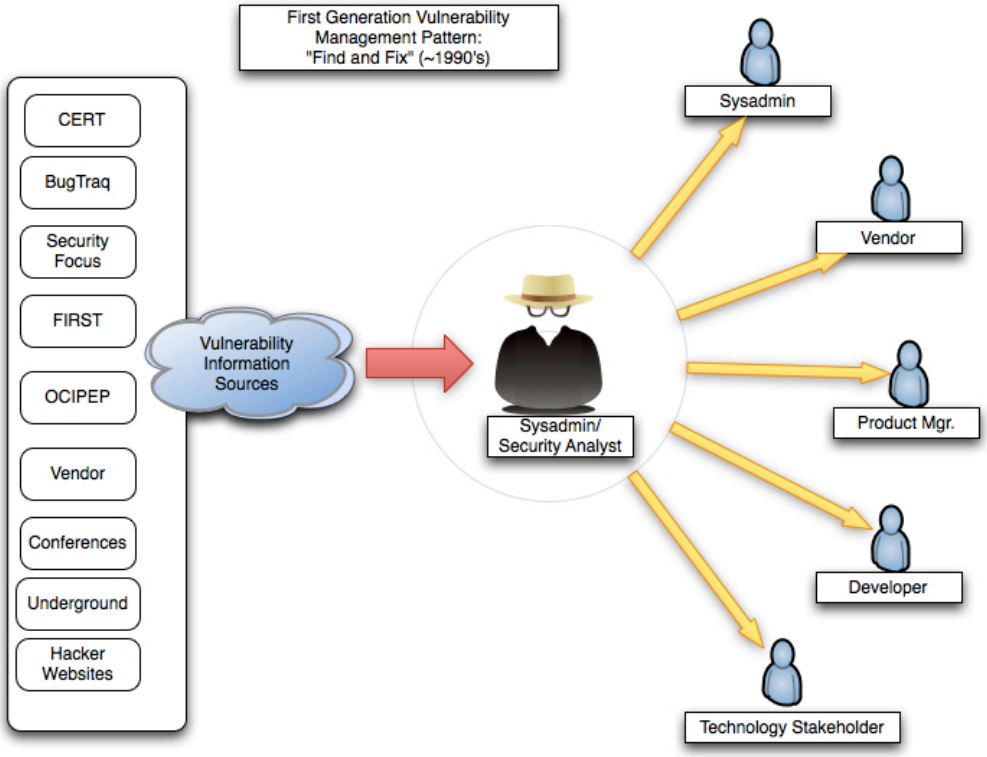


Figure 3- First Generation Vulnerability Management

3.3.1 Advantages:

This first generation “Find and Fix” pattern is agile and efficient at small scales. With adequate information, technical subject matter experts can isolate and remediate vulnerability in a system efficiently. The knowledge about the inner workings of systems also increases the level of understanding of the technologies and efforts to improve security could result in better performance and reliability. Informal networks of technical specialists emerged and facilitated information sharing via “back channels”, usually on internet e-mail lists, chat rooms and occasionally conferences.

3.3.2 Limitations:

The key weakness of the “Find and Fix” approach is that it does not scale to the scope and complexity of modern networks. The level of engineering expertise required is greater than that required for day to day operations and is very dependent upon the integrity and availability of the subject matter experts. The efficient ‘back channels’ also existed outside the governance of the owners of the networks and assets being discussed, exposing information about business operations that may have undermined strategy in some areas. The success of the pattern is dependent upon a “network effect” for information sharing, and the casual and opportunistic nature of the networks does not bear type of formal controls and information sharing agreements typically required for sharing security and operational data with external parties.

3.4 Second Generation Vulnerability Management: “Clearing House”

The second generation was the “Clearing House” pattern for vulnerability management, which was realized by the Information Protection Centre (IPC) model, and functioned as a centralized security operations department, managing information flows from organizations with intrusion detection systems, anti virus and other technologies, and advised stakeholders of patch releases. CANCERT (and later CCIRC), OCIPEP and the provincial IPCs formed the basis for this generation of cyber vulnerability management. The second generation pattern emerged primarily in the public sector, with a few private sector stakeholders. The SCADA domain was not included in this pattern because the development of a cyber-security capability was at the time still originating in IT organizations, which evolved separately from the mechanical operations divisions in which control systems resided.

Clearing houses aggregate vulnerability information from multiple sources and distribute it to stakeholders through committees, advisory services, mailing lists and conference calls. Historically, and in some rarer cases, stakeholders exchanged information via log aggregation services such as Dshield, the Internet Storm Centre, and managed security service providers. SCADA vulnerability management throughout the 2000’s conformed more to the first generation pattern than it did to the second generation pattern as it emerged in IT security.

As the volume of vulnerability information increased, pressure on IT administrators to apply patches to production systems increased and new patch management processes evolved within organizations. SCADA systems were still mostly outside the domain of IT, and so SCADA operators did not adapt to the new patch management processes, particularly because the time between patch cycles had reduced from an annual patch “roll-up” from the vendor, to monthly critical alerts. In many organizations surveyed, the new IT processes did not account for time required for testing and QA that would meet engineering standards for SCADA systems.

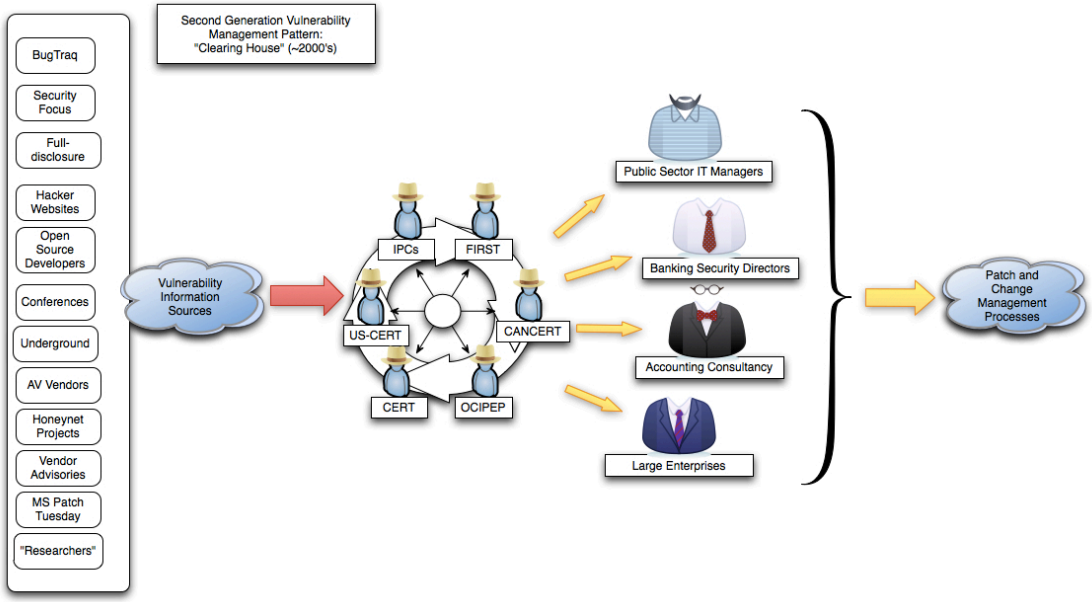


Figure 4- Second Generation Vulnerability Management

3.4.1 Advantages:

The key advantage to the clearing house pattern is the identification and development of formal networks of stakeholders. Clearing houses can scale the niche expertise required for evaluating vulnerability information by adding stakeholders and customers for the information product. The pattern requires an agile patch management process in participating organizations and it has driven the adoption of formal IT security practices in diverse and unrelated sectors. The relationships between clearing houses and stakeholders enabled them to broker trust and to facilitate further information sharing and security partnerships. The resultant networks enabled the proliferation of security best practices and the coordination of incident response to global internet events related to virus and internet worm outbreaks.

3.4.2 Limitations:

The key limitation of the clearing house pattern has been the volume and variable quality of vulnerability alert information generated. The model created new costs for organizations to keep up with the flow of alerts and subject matter experts to evaluate the criticality of each new advisory. The increased rate of patch management requires participants to be in a constant reactionary mode. There is very little integration or automation in

the testing and assessment of the information supplied by clearing houses. Participants in the pattern must manually analyze assess their exposure to the vulnerability based on the information from the clearing house. The limitations in the clearing house model resulted in limited adoption, particularly in the SCADA space, where developers had made engineering decisions based on assumptions about the level of environmental change that should be anticipated in their solutions. These assumptions did not anticipate how dynamic networked environments would become.

3.5 Third Generation Vulnerability Management: "Enterprise Vulnerability Management"

The third generation of vulnerability management solutions is automated, decentralized and continuous. Point-in-time network scanning for vulnerabilities evolved throughout the 2000's into differential scanning. The key development was that organizations began to record and analyze changes in security scan results over time. In concert with pervasive intrusion detection and prevention systems and anti-virus and other host based sensors, a complete picture of the security posture of an organization began to emerge.

The Security Event and Incident Management (SEIM) specialty emerged with the capability of aggregating log data from multiple sources in the enterprise network. When coupled with a differential security scanning feature, a dynamic dashboard of real time security posture provides views to systems administrators, IT governance, risk management and certification and accreditation authorities in the organization. Dashboards for SCADA functionality are an integral part of a control system, where the Human Machine Interface (HMI) provides current information about operational parameters. In this regard, SCADA solutions have been ahead of the curve, visualizing real time information about the state of the system. However, so far, information security has not been a key part of these displays.

SEIM solutions are able to receive alerts from HMIs and other SCADA components, since they are designed to integrate diverse types of data using simple data transformation and adapter interfaces. The challenge has been with the continuous differential vulnerability scanning aspect of the solutions.

Since SCADA systems use embedded or proprietary OEM versions of commercial and open source software, they diverge from the main distribution of the product, often making it incompatible with or disconnected from the main patch management cycle of the product. Security vulnerabilities that are fixed in mainstream distributions remain open in the embedded and OEM versions and they have been inadvertently triggered by the probe messages of network scanners.

The third generation pattern emerged in the middle of the decade, but it has taken some time to be accepted by markets beyond early adopters. The evolution of new security scanning technologies in some cases did more to isolate SCADA systems than to bring them into the security fold. It was common for network security scanners to cause control systems to fail unexpectedly, causing malfunctions in the machinery connected to it. As a result, many surveyed SCADA operators have so far resisted the implementation of advanced security controls and technologies on their systems due to reliability and safety concerns.

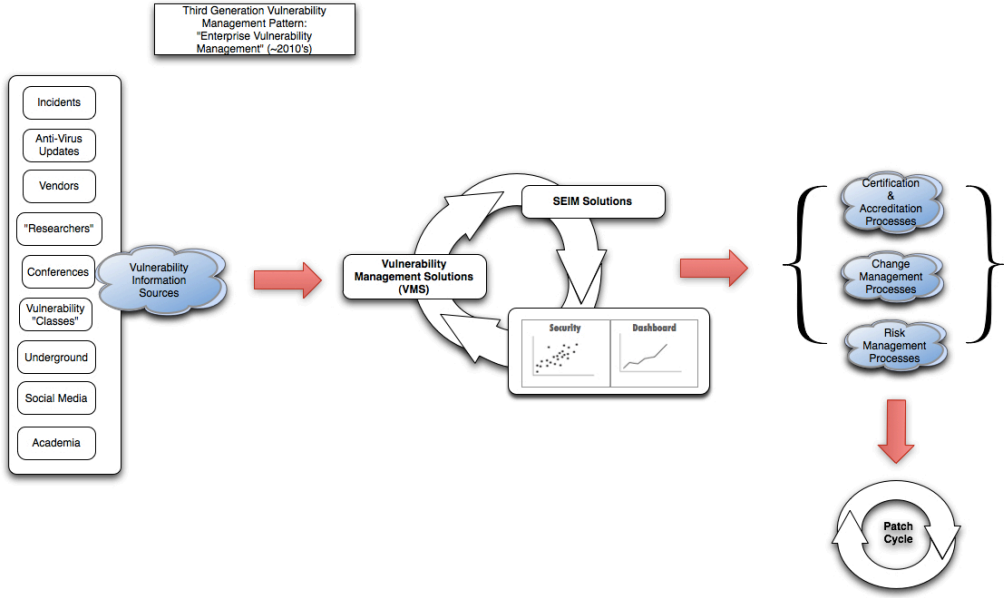


Figure 5- Third Generation Vulnerability Management

3.5.1 Advantages:

Enterprise vulnerability management solutions are comprehensive, automated, dynamic and timely. They provide an up to the moment view of the security posture of the network, and management tools for monitoring change in organizational security performance over time. They provide a dynamic and authoritative inventory of networked assets. For a given vulnerability, a list of unpatched or unprotected systems can be derived within seconds. Specialist expertise in the assessment of system vulnerabilities is centralized in the VMS vendor lab, and the expertise required by organizations to process the reports from the VMS is significantly less specialized, and more widely available.

3.5.2 Limitations:

The key limitation of enterprise VMS with regard to SCADA systems is the fragility of embedded operating systems and applications. Recent security research and development has focused more on SCADA and VMS products will necessarily improve, however the level of trust in network scanners from SCADA operators is not high. The risk from network scanners is the result of a very high likelihood and impact of SCADA system failures caused by scan activity.

3.6 Next Generation Threat/Vulnerability Management (SCADA): A Hybrid Approach

The Next Generation vulnerability management system should be a hybrid that emphasizes the organizational co-operation of the second generation "clearing house" pattern and enables the visibility, depth and technical sophistication of the third generation "enterprise vulnerability management" pattern.

The requirements for a SCADA Cyber Threat and Vulnerability Management System imply the integration of threat analysis with vulnerability management. In the research performed for this study and conducted as a part of ongoing work, the study team found that the vulnerabilities in SCADA systems are often functionally identical to those in regular IT systems. The classes of vulnerabilities are the same, and in many cases, the vulnerabilities themselves have been discovered in mainstream systems, and left unpatched in embedded control systems because of their divergent software development lifecycles.

SCADA operators and critical infrastructure asset owners have IT processes that are developing maturity at a normal rate. The integration of SCADA systems into IT governance processes is already underway in many larger organizations, and it is foreseeable that the VMS vendors will adapt to the demand for safer, more reliable scanning techniques as more SCADA operators go to market for security solutions. What has distinguished SCADA security from the mainstream is the threat model and the resultant risks, which are related to health, safety and strategic interests more than to business integrity and continuity. Unlike telephone, internet, cable and cellular communications companies, critical infrastructure providers are more diverse and numerous in Canada. The myriad of municipal water management companies, power generators and distributors, transportation network operators and energy suppliers has so far defied consolidation under a single security umbrella.

In spite of its evident limitations, a clearing house approach to vulnerability management in these sectors should be a part of the solution. First, Canada should establish a foundation for a network of stakeholders, which will provide a channel for education and for enrollment into their shared stewardship role in the security of national infrastructure. An exercise that determines the sectors, infrastructure, companies, organizations and contacts for national critical infrastructure in Canada would enumerate the constituency of stakeholders and illuminate further requirements for a clearing house capability to serve them.

Existing organizations such as the Canadian Cyber Incident Response Centre (CCIRC); the Information Protection Centres (IPC) in each of the provincial governments; and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at the U.S. Department of Homeland Security (DHS) provide a model for modern threat and vulnerability information clearing houses. While the models and technologies exist, the networks of relationships do not.

Whether threats have cyber capabilities or not, analysis of the dynamic economy of interests and opportunities for threat agents is well within the existing mandate of Canada's security agencies. The key to a SCADA cyber threat and vulnerability management system is to find the pivot points for integration of the threat environment and technical vulnerability information. Demand for technical vulnerability information has driven a strong market for IT security solutions, with Canadian companies among some of the leaders in the space. Gaps in the vulnerability information field are filled quickly by competing researchers, companies, conferences and academics. Processing the volume of vulnerability information is a more pertinent problem then generating it.

The unique need implied by SCADA security is that an integration layer is required between critical infrastructure asset owners who already have access to vulnerability data, and the security agencies that can contextualize the data with current, strategic threat information. Clearinghouses have the capability to provide this layer since they may act as both a trusted proxy and an integrator for threat and vulnerability information.

The technical vulnerability management component will be a function of the maturity of IT security controls in the specific industry sector. The approach to SCADA system vulnerability by organizations surveyed as a part of this study conformed to first generation "Find and Fix" patterns.

IN this model, a technical SME capability was responsible for responding in an ad hoc manner to emerging threats, and in more advanced organizations, deep technical security analysis was contracted to specialists as a part of the procurement and development of new control system solutions. However, even in organizations that deployed it in their IT environments, continuous, differential management of threats and vulnerabilities in control systems was not practiced.

A next generation solution would rely on state of the art enterprise vulnerability management and SEIM solutions to be functional in SCADA environments. Threat information from law enforcement and the IC could be filtered through clearing houses and provided to critical infrastructure asset owners, who would use it to filter information from their technical vulnerability management solutions. Asset owners could then share derivatives of the risk information, refined as a result of their own vulnerability information in the context of threats, with the clearing house for distribution to IC and law enforcement stakeholders.

A sample pattern for a Next Generation Cyber Threat and Vulnerability Management system is included below. The example flow in the diagram begins with threat data being received by the IC and law enforcement stakeholders from global situation reports. The data is processed into Threat Intelligence, and distributed to clearing house partners. The partners included in the example are for illustration purposes, since the capability will remain necessary, but the organizations may change.

A key point is the relationship between the IPCs and municipalities. Since municipalities receive payments from provincial governments, and many of them have significant public hydro-electric, transportation networks, aviation authorities and water treatment facilities, it was pertinent to raise the opportunity to engage municipalities via the network of IPCs, since transfer payment agencies and other direct channels between them may already exist. Some provincial emergency management organizations are known to have some links to asset owners, however the expertise for vulnerability management is a corporate function, hence the need for a channel to between the owners and the centres of expertise.

The Asset Owners are represented as critical infrastructure domains, which comprise SCADA system operators in a variety of sectors. As the network of owners and the clearing houses becomes more populated, the value of any new owner joining will increase as a network effect.

An asset owner that has an enterprise vulnerability management solution, whether in house, or as a service, is able to produce cyber risk intelligence in exchange for threat intelligence (used to improve their security posture.)

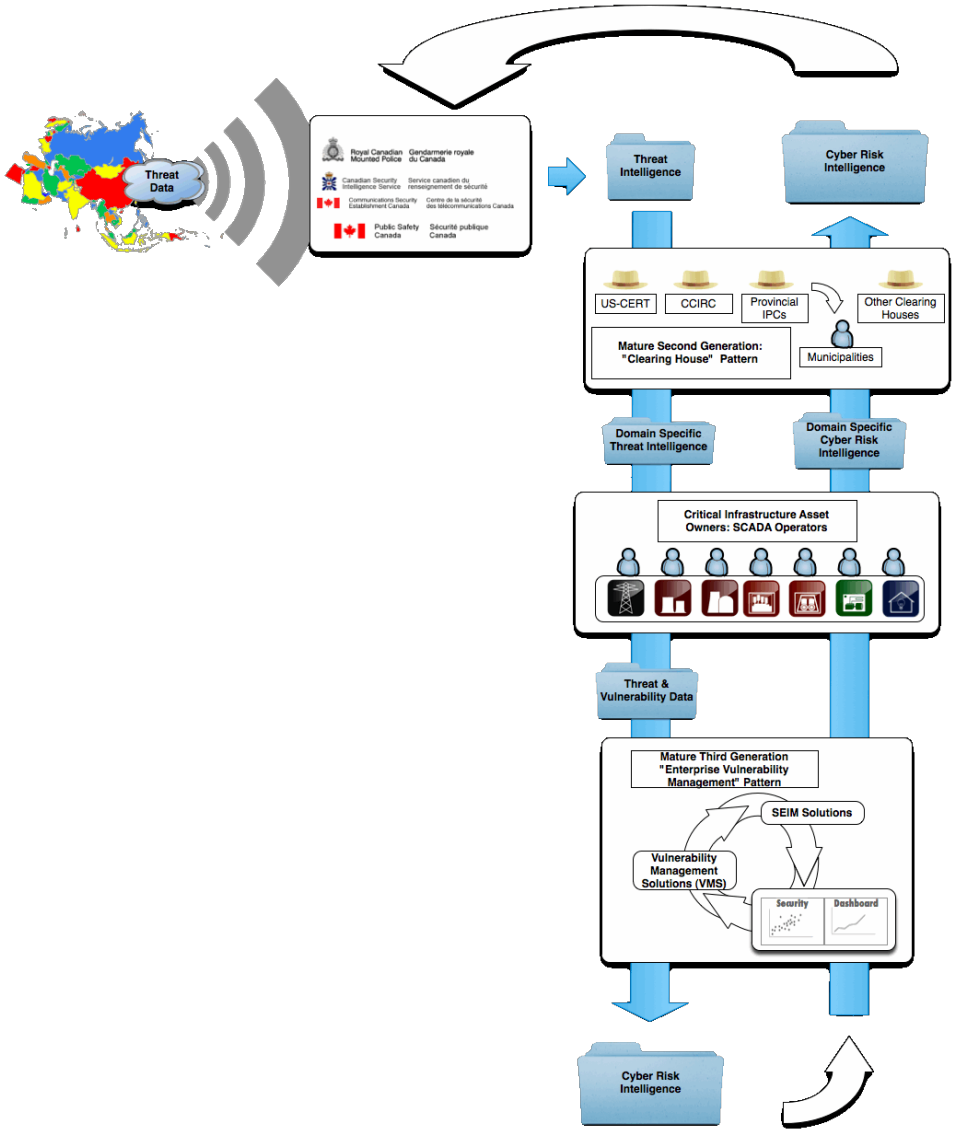


Figure 6- Next Generation Vulnerability Management

3.7 Conclusions

The key conclusion of this study is that the technology for a robust cyber vulnerability management solution exists, however the network of relationships required to implement it as a national infrastructure protection capability, as of yet, does not. Enterprise vulnerability management solutions must improve their ability to meet the needs and sensitivities of SCADA systems. In turn, SCADA system vendors must improve their software development lifecycle security so that they are at least as robust at off the shelf IT solutions.

The study showed that effective threat and vulnerability management systems are not dedicated solely to the understanding of the threats and vulnerabilities themselves, but rather they support how information is used to provide support for a proactive (protection) and reactive (recovery) lifecycle. In addition, the study showed that the best approach for a SCADA cyber threat and vulnerability management system incorporates features and characteristics of past management frameworks, and that certain aspects of traditional management frameworks can work well in future-state strategies. The key to a SCADA cyber threat and vulnerability management system is to find the pivot points for integration of the threat environment and technical vulnerability information.

In spite of its evident limitations, a 'clearing house' approach to vulnerability management in these sectors should be a part of the solution. Canada should establish a foundation for a network of stakeholders, which will provide a channel for education and for enrollment into their shared stewardship role in the security of national infrastructure. An exercise that determines the sectors, infrastructure, companies, organizations and contacts for national critical infrastructure in Canada would enumerate the constituency of stakeholders and illuminate further requirements for a clearing house capability to serve them.

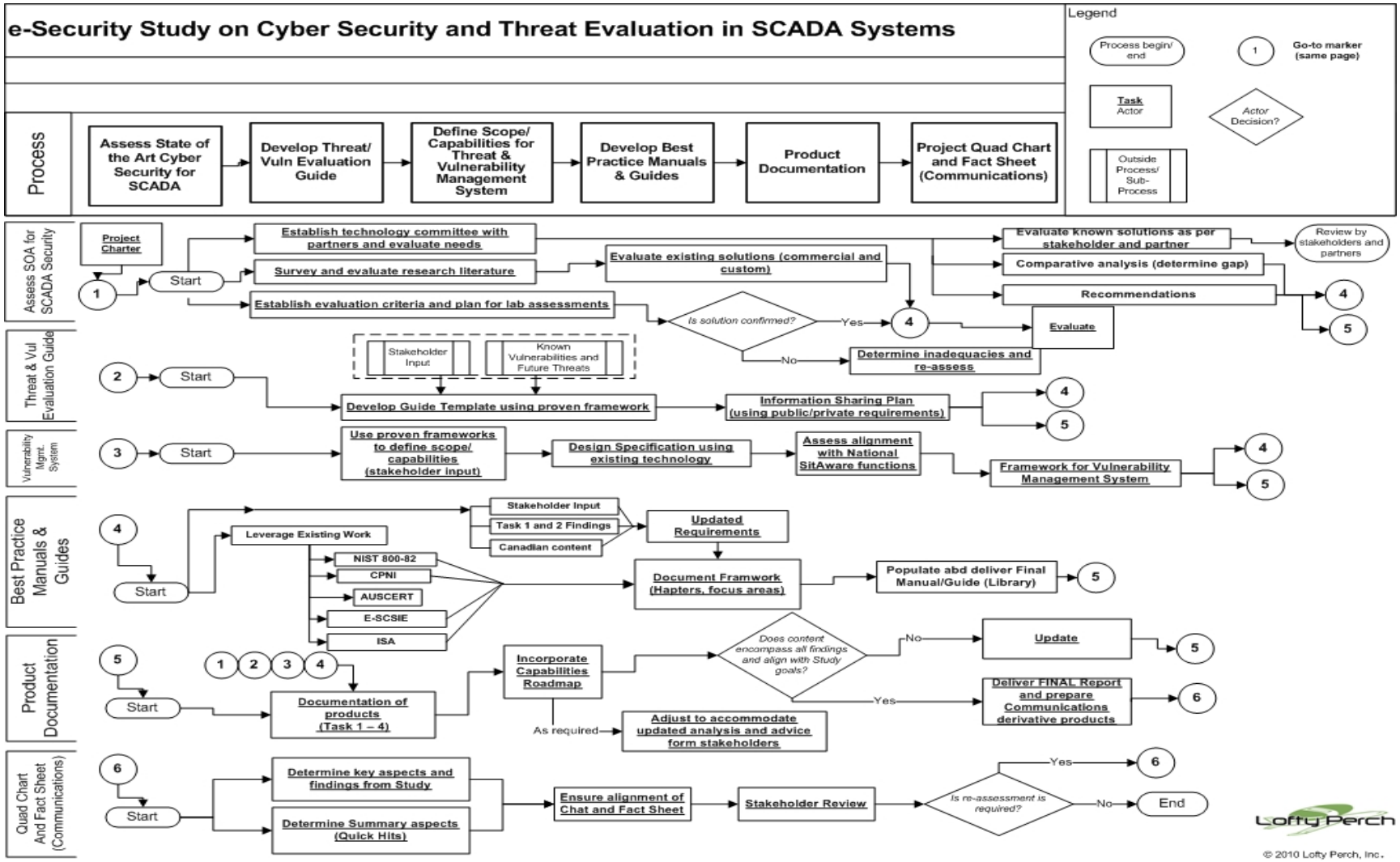
The unique need implied by SCADA security is that an integration layer is required between critical infrastructure asset owners who already have access to vulnerability data, and the security agencies that can contextualize the data with current, strategic threat information. Clearinghouses have the capability to provide this layer since they may act as both a trusted proxy and an integrator for threat and vulnerability information.

The technical vulnerability management component will be a function of the maturity of IT security controls in the specific industry sector. The approach to SCADA system vulnerability by organizations surveyed as a part of this study conformed to first generation "Find and Fix" patterns. A next generation solution would rely on find and fix approaches as well as state of the art enterprise vulnerability management and SEIM solutions to be functional in SCADA environments. Threat information from law enforcement and the IC could be filtered through clearing houses and provided to critical infrastructure asset owners, who would use it to filter information from their technical vulnerability management solutions. Asset owners could then share derivatives of the risk information, refined as a result of their own vulnerability information in the context of threats, with the clearing house for distribution to IC and law enforcement stakeholders.

The vulnerability of infrastructure in Canada would be reduced by the implementation of an approved SCADA solution products list similar to the Common Criteria "Certified Products"[19] list.

[19] http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html

Annex L Project workflow



4 Introduction Task 4 – Produce a Best Practices Security Manual or Guide

This document provides a comprehensive report on specific tasking as it pertains to Project Task 4 – Produce a Best Practices Security Manual or Guide. The tasking in this project area was developed to provide a set of best practices to Canadian critical infrastructure asset owners for managing the security of their SCADA and control systems. It is intended that this work will enhance the resilience of Canada's critical infrastructure by providing recommended best security practices to asset owners. The tasking was completed following several key strategies:

- Evaluate and leverage existing work done by the global community of interest and cross correlate with the findings and observables from previous study activities

- Review functional security characteristics between SCADA and traditional IT strategies and incorporate stakeholder input into requirements set to reflect Canadian interests

The study team performed a comprehensive review of existing literature regarding SCADA security best practices and guidance, and incorporated feedback based on interactions with study partners and real-world assessment /training activities performed by the study team. It is important to recognize, however, that the current landscape of best practices and security guidance for SCADA is rarely country specific, and that the current compendium of usable guidance offers Canadian asset owners a tremendous amount of choice when developing security strategies for their control systems. Based on the study teams extensive interaction with asset owners, and their own experience in the development of many of the contemporary standards and recommended SCADA practices, the study team ensured research value by providing the reader insight and direction for what is currently perceived to be the most timely and useful information. A comprehensive set of references has also been developed and is included here.

This document is intended to provide content to be used in the comprehensive material to be delivered in the Final Project Study Report. The material in this document will, where possible, reference other study activities so that the reader will be able to interpret and leverage the information efficiently.

4.1 Description of tasking and subtasking activities

The primary task element, as a function of the overall study methodology, is shown in figure 2 below. This is derived from the comprehensive Study Workflow as shown in Appendix A.

Figure 2 - Detailed workflow for Task 4

The core activities of this task involved the establishment of a well defined review committee of subject matter experts and partners who had specific interest and capability in the area of developing

recommended practices and guidance for securing SCADA systems and Industrial Control Systems (ICS). The study performed a comprehensive review of existing literature specific to the tasking focus area, and included recommended practices and standards from (selected list):

- NIST
- DHS Catalogue of Control Systems Security: Recommendations for Standards Developers
- DHS CSSP Procurement Language Documentation
- DHS CSSP Control Systems Security Program Library
- DHS CSET Evaluation Toolkit Library and support documentation
- CPNI
- ISA (SP-99)
- E-SCISE
- AMI-SEC
- NISTIR
- AUS Attorney General
- AGA
- INGAA
- DoT
- U.S. TSA
- API
- NERC, FERC, NRC
- U.S. DoE (INL Comparison of Cross-sector Cyber Security Standards, etc)

Regarding previous work, the study team looked very closely at the results from other tasking areas and reviewed emerging best practices arising in the general SCADA community of interest. Where appropriate, the study team emphasized the approach to address unique requirements from the Canadian stakeholder community. The resulting material provides an overview of select ideas and approaches that can help asset owners shape resilient security plans for Canadian SCADA and control systems.

4.2 Guidance

Control systems are automated systems which, when working together, manage a physical process. Examples of physical processes can include electricity generation, transmission and management; automotive manufacturing; chemical processing; oil refinement; liquid pipelines; water treatment and fresh water distribution; traffic control; airfield lighting and landing systems. Any process that has a physical component, that moves, heats, cools, mixes, pumps an object or objects, will most likely use control systems to do it.

In contrast, traditional information systems manage information. Information is collected, stored, mined, analyzed, reformatted, manipulated, and presented to one or more audiences for the purpose of decision making. Information systems do not necessarily cause physical actions in the physical world without the intervention of a human actor. Even the robot in a backup system in an informatics data center that swaps backup tapes is considered a control system, because it physically sorts and replaces backup tapes without human intervention. Database servers, application servers, workstations, enterprise resource planning (ERP), data storage systems are all examples of information systems.

Despite this difference, information systems and control systems are converging at a rapid pace. Once isolated from each other, this new connectivity is primarily the result of the need for business leaders to quickly and efficiently acquire access to information about the processes they manage. Just-In-Time

(JIT) manufacturing is one example of why a corporate audience now requires up-to-the-minute information about processes. Market fluctuations which impact demand and changes in the supply chain have immediate effects on the volume or the configuration of the products that manufacturers make. Another example is the electrical sector, where centralized market information about consumption determines payment to suppliers, which in turn will cause a generation company to alter their generation volumes in almost-real time. Business information, the province of information technology, is now an immediate determining factor in how physical processes are managed. Information management systems have found their way into control system environments to manage that data. As such, depending on the sector or business, the protection of critical control systems can be a matter of national and economic security

In some industries the market regulator requires immediate access to information about a company's supply capabilities so that they may manage the broader market. The best example is, again, the electrical sector. In the supply of electricity, surplus production cannot be allowed to occur. Generation and consumption of electricity must balance to keep the bulk power system operating. When generation and consumption of electricity are not in balance, either equipment is damaged or blackouts occur. Load balancing requires intimate knowledge of the state of the bulk power system, so load balancing authorities require real-time information concerning the state of the equipment of all the major electricity asset owners, such as generating companies and transmission companies.

When business leaders, business partners, or regulators need access to information about the state and function of a process, these new audiences for this information require that control system networks and information system networks both connect and converge. Control systems which were traditionally separated physically from corporate systems are now connected to these networks to provide access for business decision making. Historical information about the process must be stored for analysis, requiring the presence of database servers, traditionally an IT function. Various audiences need to view process state information in various forms, requiring some form of presentation application. This will be done using either a client/server application or web-based application, which has also been traditionally managed by IT departments. Modern network appliances and services, again traditionally an IT domain, are being used increasingly in control systems environments to improve communications reliability and speed and to connect control systems with business systems.

Controls systems and information systems are connecting and converging. As a result, risks associated with information systems are now moving into the control system domain, and those new risks have to be managed.

4.3 Security Basics

When we speak of the security of a system or process, we are really referring to the relative value of a set of security properties present in the system or process. Every asset, whether it is an information asset or a physical asset, can have a defined set of security requirements. Strategic plans may have a strong requirement for confidentiality. Billing data may have a strong requirement for integrity and confidentiality. Market information may have a strong requirement for integrity and availability. In the case of industrial control systems, the systems managing a critical process for business will always have a very strong requirement for availability.

There are other security properties. The following table shows common security properties of information and system assets, and their definition.

Property	Definition	Information	System/ Process
Confidentiality	A property describing the capability to keep information secret	X	

	or restrict knowledge of the information to a pre-defined set of accepted individuals or systems or processes.		
Integrity	A property describing the capability to ensure that information sets or processes have not been altered.	X	X
Availability	A property describing the capability to ensure that information is available to its intended audience, or that processes run without failure.	X	X
Authenticity	A property describing the validity or genuineness of an information set.	X	
Non-repudiability	A property which ensures that the receipt or sending of information cannot be denied by the person or process which sent or received the information, or that a person or process cannot deny an action taken.	X	X
Reliability	A property describing the capability for a process to invariably arrive at the same result with the same inputs. (Reliability in data sets is equivalent to integrity)		X
Accountability	A property describing the level of assurance that an information set or process has an accountable owner.	X	X

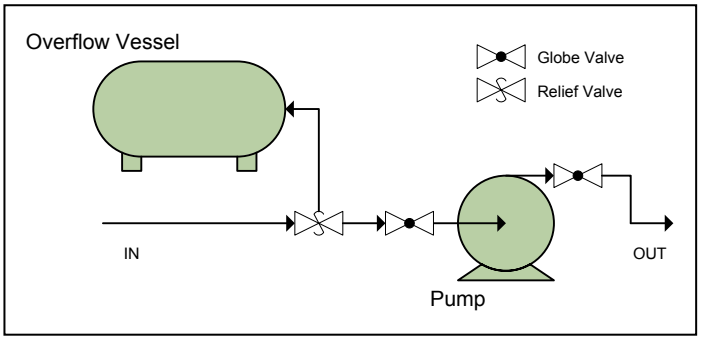
When examining a data set, system or process, the asset will have a requirement for some level of assurance of these security properties. Note that confidentiality, integrity and availability are highlighted. This is due to the fact that most security professionals use these properties to determine the security requirements for information systems and control systems. As previously mentioned, strategic planning information requires a high level of assurance of confidentiality and integrity, but may require only a moderate level of assurance of availability. Asset classification is the process of determining what the required level of assurance for each of these security properties is appropriate for that particular asset.

In order to perform asset classification, some pre-requisites must be met.

- All the assets must be enumerated and catalogued.
- An impact analysis must be performed on each asset or asset class.

The requirements of the asset or asset class are determined by the impact analysis. Depending on the level of impact of a failure (or other negative consequence) on the asset, the requirement for the level of assurance of being able to provide those security properties is determined. Impacts can include loss of revenue, replacement and repair costs, injury or death, loss of reputation, and opportunity costs.

Let us examine an oil pipeline. We will consider only one section of pipeline between two pumping stations and the stations and their components. For the purpose of this example, we shall say that at each pumping station, there is a valve on either side of the pump to isolate the pump, and there is a pressure relief valve upstream from the pump and its isolation valves. The relief valve is triggered by excess pressure in the line, which then diverts product into an overflow vessel.



Should the valve which is downstream from the pump close while the pump is still running, the pump could be damaged, and/or the pipe between the pump and the valve could rupture. The relief valve should then trigger due to pressure build-up in the line, and

oil should then be diverted to the overflow vessel. If the upstream pumping stations are not turned off, or if the inbound oil is not diverted to a secondary pipeline, the overflow vessel will continue to fill until it in turn overflows. Impacts could include:

1. Damage to equipment (repair costs)
2. Lost revenue
3. Environmental impact (spill from the overflow vessel)
4. Reputation damage

The impacts to an organization due to equipment failure are well understood by their control systems engineers and their management staff. Therefore it should be easy to define the security requirements for the pumping station equipment and the control data used to manage them.

Security Properties of Pumping Equipment	Impact due to failure of property	Required Assurance
Confidentiality	N/A	Low
Integrity	Command data failure could cause equipment failures	High
Availability	Any device not being available to perform its function, at a minimum, causes loss of productivity	High
Authenticity	Rogue system or agent that could inject commands to cause any failures, leading to any of the possible impacts of pumping station failures	High
Non-repudiability	Inability to identify the perpetrating process or individual	Medium
Reliability	Any device not being available to perform its function, at a minimum, causes loss of productivity	High
Accountability	N/A	Medium

The required assurance level for each property will be appropriate to the organization, based on an impact analysis. Whether that impact analysis is quantitative or qualitative or both, the purpose here is to develop a graduated set of security property requirements for each asset or asset class. This will allow the later matching of appropriate control sets to the assets based on their requirements.

Alternately, the required security assurance level can be reduced to a single value – high, medium or low. Examination of the NIST 800-53 standard shows just that approach. The asset or asset class has a single security assurance requirement, and controls are selected based on that single value. This simplifies the model for ease of use. However, most security controls provide assurance for only a subset of security properties, not all of them. So matching controls to requirements more granularly creates a more efficient and robust control set. It is left to organizations to determine what level of granularity is appropriate for their business and SCADA operational environment.

4.3.1 Security Standards of Good Practice

There are many standards of good practice to choose from when examining how to manage security risks in control systems environments. In fact, numerous organizations have created case studies that focus on the use of diversified standards for SCADA domains. During the course of the study, the study team was engaged in several risk and compliance assessments for SCADA systems, and used a variety of well-known standards in their work. Understanding these standards will allow asset owners to create and manage a program to mitigate cyber security risks in their control systems environments. When an asset owner is without formal direction to adhere to a certain security standard or practice, these standards allow for great flexibility to accommodate for the unique challenges presented by control system environments.

4.3.2 ISO 27001, 27002

The ISO 27001 and 27002 standards ensure proper security processes and technology are implemented in information systems. The 27001 standard describes an information security management system, or security program management process. This process includes creation and maintenance of security policies; threat and risk assessments; protection and prevention activities; consequence management; and evaluation and oversight of the entire management process. The ISO 27002 standard describes a list of actions or activities to undertake to improve the security of the organization. This is fairly comprehensive list of activities, many of which are interrelated:

1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management

7. Access Control

8. Information Systems Acquisition, Development and Maintenance

9. Information Security Incident Management

10. Business Continuity Management

11. Compliance

NERC CIP

The North American Electricity Reliability Corporation (NERC) is responsible for maintaining the reliability of the bulk power system for North America. This organization is comprised of the major electricity providers in North America. NERC is the regulatory body made up of the regulated entities, creating a self-regulatory framework for the electrical sector.

NERC has a series of standards targeting the reliability of the bulk power system, including those for Engineering specifications, Incident Reporting, Emergency Preparedness, Critical Infrastructure Protection, Facilities Design, and Communications. The Critical Infrastructure Protection standards are those which govern cyber security for organizations managing the North American Bulk Power System (BPS).

The NERC standard is very similar to the ISO 27002 standard, and thus has some good applicability to SCADA and control system operations. Allowance has been made for the special needs of control systems, in that the set of controls recognizes the primacy of availability, reliability and predictability in the set of security properties of systems. Security properties such as confidentiality and non-repudiation have a lower priority in ICS environments.

The following list shows the different NERC CIP standards:

002: Critical Cyber Asset Identification

003: Security Management Controls

004: Personnel & Training

005: Electronic Security Perimeters

006: Physical Security of Critical Cyber Assets

007: Systems Security Management

008: Incident Reporting and Response Planning

009: Recovery Plans for Critical Cyber Assets

Within each standard is a set of required controls which electricity asset owners are obligated to implement in their ICS environments

4.3.3 NIST 800-53, 800-82

The National Institute of Standards and Technologies (NIST) provide a series of standards for computer and information security. NIST standards are designed for US federal government computer systems but have extensive applicability to SCADA systems as well. In many cases US federal government agencies are mandated to ensure that their systems comply with these standards. However, they are publicly available for use by all. Referenced as the 'Special Publication Series', or SP 800 series, these standards range from basic input/output security to specific guidelines for SCADA/ ICS security. Of particular interest are the two standards SP 800-53 and SP 800-82.

SP 800-53 is called "Recommended Security Controls for Federal Information Systems and Organizations". This document provides a guide for the protection of information and information systems, and facilitates its aims by:

1. Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;

2. Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems;

3. Providing a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies;

4. Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and

5. Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

Of interest in this standard is the introduction of security assurance levels. Information data sets and systems are analyzed and categorized according to the impact of failure. The magnitude of this impact sets a required assurance level for that information data set or that system. Controls are applied to that system or data set based on its specified assurance level – higher assurance requirements demand more controls or more powerful controls. Another point of interest is the introduction of the notion of compensating controls. This notion allows the substitution of controls when certain controls are not able to be used on some systems, whether due to technical or operational limitations. Appendix F of the SP 800-53 contains a catalogue of system controls in different control families for use on information systems. Appendix I in SP 800-53 describes control substitutions appropriate for industrial automation and SCADA systems.

The SP 800-82 standard is a more recent standard aimed specifically at industrial control systems, and has proven to be exceptionally useful to the community of interest. The framework is similar to SP 800-53, but specifically targets control systems, accounting for the special needs of control systems. In addition to providing a catalogue of security controls for ICS, this standard includes a discussion of ICS components and how

they differ from traditional IT systems, differentiated threats and risks in ICS environments, and a discussion around building a business case for security in ICS environments. As the material was developed through a collaborative effort involving asset owners, SCADA engineers, security experts, and researchers it has very specific guidance that is derived from real world lessons learned.

The controls in SP 800-82 are derived almost entirely from other NIST standards. But where 800-53 lists technical and process controls for individual information systems, 800-82 references many other standards to build a more comprehensive set of managerial controls as well. 800-82 refers to 800-53 extensively for technical controls, but also refers to standards such as 800-12 on security policies and procedures, 800-23 on the acquisition of systems, 800-35 on security services, 800-64 on inclusion of security in development lifecycles, 800-65 on including security consideration in capital planning, and others.

4.3.4 Others

NRC 5.71 – controls required by the Nuclear Regulatory Commission to be implemented in all US based nuclear facilities.

ISA SP-99 – originally conceived by the International Society of Automation as a series of standards, parts of which were aimed at different audiences – the asset owner, integrators, and vendors. Now it is an independent set of 3 standards which resemble the ISO/IEC 27001 and 27002 standards.

ISO/IEC 15408 (Common Criteria) v3.0 – A framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

DoDI 8500.2 – DoD instruction on implementing controls for information assurance

CSA Z246.1 – This Standard uses the concept of a security management program, and in particular risk management, to address security issues in petroleum and natural gas industry systems.

API 1164 – A pipeline SCADA security standard.

INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry – provides guidance on addressing the control system cyber security plans section of the natural gas pipeline operators' TSA required CSP.

4.4 Security Management

4.4.1 Ownership and Authority

A well run organization formally assigns responsibilities to its managers to ensure that all operations are overseen by experienced, skilled supervisors. Security of control systems and information systems is a complex task, requiring careful oversight. An executive manager must be formally assigned the responsibility of managing security controls within the organization. This individual is tasked with ensuring that appropriate security controls are in place to manage the security of the organization. Further, this individual is responsible for ensuring that measurement of security capabilities and outstanding risks can be performed, and are performed regularly to provide security performance information to other managing stakeholders.

Sample list of responsibilities, as envisioned by ISO/IEC 27002:

- ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes;
- formulate, review, and approve information security policy;
- review the effectiveness of the implementation of the information security policy;
- provide clear direction and visible management support for security initiatives;
- provide the resources needed for information security;
- approve assignment of specific roles and responsibilities for information security across the organization;
- initiate plans and programs to maintain information security awareness; and
- ensure that the implementation of information security controls is co-ordinated across the organization.

4.4.2 Policy

A well formulated security policy is an indicator of organizational commitment to security. It sets out the security objectives of the organization – such as the risk framework adopted by the organization, and standards and regulations to which the organization is obligated to adhere. This is then published for all to see. This is important to create a culture of responsibility for security. Without a good security policy, it is impossible to align day to day procedures and practices with organizational security objectives.

It is important to remember that good security is about identifying and managing risks. A security policy is required to document a framework for risk management and risk acceptance. It also lays out the roles and responsibilities for the security manager or managers. The traditional approach in IT was straightforward, but the control system domain can create situations where policies can be modified to accommodate for stringent operational requirements. These policies should be reviewed periodically for applicability and effectiveness, for any changes to its components, or how the granularity of the policy can be updated to accommodate for SCADA and control system requirements.

4.4.3 Least Privilege

The principle of least privilege applies not only to users accessing files on computer systems, but every aspect of access control management. Communications on networks can be governed by the same principle when attempting to control communications. Allow only those communications necessary to support the business purpose or mission objectives. It can apply to automated processes, whether virtual or physical. Only permit an automated process to have access to functions or information that are relevant to its purpose.

Use of the principle of least privilege implies some preconditions, some of which cannot be met in contemporary SCADA environments. Although these conditions have obvious benefit when enforced, some of them are a function of the vendor solution, thus prohibiting the asset owner from being able to implement them.

- Sources of action, or subjects, are well defined. All users are known, all systems are known, all processes are known.
- Targets of action, or objects, are well defined. Systems and their components are well known. Data sets are well known. Object processes are well known.
- Subjects' identities can be positively authenticated.
- The function of all subjects, and the activities that they require permission to do in order to fulfill their functions, are well defined.

This principle, when applied properly, is an extremely powerful security tool. By limiting the activities that subjects are allowed to perform to only those required to support their functions, the opportunity for abuse of information systems is reduced to the minimum possible.

The only way to improve on the principle of least privilege to reduce opportunities for abuse is to redefine the roles and responsibilities of all subjects to reduce functional overlap to the minimum necessary for proper operations and appropriate redundancy. But roles and responsibility of personnel within the ICS domain are not always clear, and numerous scenarios can be created to illustrate conditions when users cannot be bound by least privilege (i.e. duress or emergency conditions).

4.4.4 Asset Identification and Classification

In order to select an appropriate set of controls for an asset, whether that asset is an information asset, a physical asset, or a process, one must have an understanding of the security requirements of the asset. The security requirements of the asset are based on the likely business impact if the asset fails to perform its intended purpose, or could contribute to the failure of other assets. The section above entitled “Security Basics” describes a model for determining security assurance requirements for assets.

It is stated that all assets need to be catalogued and a set of security assurance requirements for each asset or asset class must be developed based on and appropriate impact analysis. If tying security assurance requirements to an asset class rather than to each and every asset, every asset must be declared as belonging to a particular asset class to inherit its security assurance requirements from that class.

4.4.5 Security Services Model

In security assurance requirements, impact analysis is used to determine the requirements that information sets or processes have for specific security properties. In the security services model an environment is designed to provide those assurance levels.

This is a complicated and sophisticated addition to the notion of security assurance requirements. To design an environment or system which can provide high confidentiality, or moderate availability, or high integrity, all the possible ways in which that security property can be compromised must be determined and controls put in place to prevent all of them. In the long run it is more efficient because an organization which provides environments or systems or processes with particular assurance levels has pre-determined how they will manage all aspects of service provisioning. Further, most Information Technology groups in organizations are familiar with this model, as most other types of IT properties are provisioned in this manner. Uptime guarantees, turnaround times on updates and fixes, storage performance, system performance, application performance – these properties are designed into provisioning of IT as a service. This same model can be extended to the provision of security assurance. Or more accurately, security services can be included in the service provision model.

Control catalogues, such as CoBIT and NIST 800-53, make excellent starting points. If an organization has already expanded their control catalogues to handle multiple security properties, even better. Designing systems and network architectures using the controls catalogue, without regard to individual systems and processes which will use them, allows a company to pre-determine how they will provide controls to meet security assurance requirements of various assets or asset classes. Then when an asset is determined to require a certain security assurance level, it can be deployed into a pre-existing environment designed to provide them. All development processes, project management processes, and

ongoing management processes will also be pre-determined, and controls will already be in place to appropriately manage and secure the asset according to its security requirements.

Some example pre-existing controls can include:

- Assets with high availability requirements have hot spare systems in place in case of failure of primary systems. In the case of a computer system, a duplicate system has been set aside and is kept up to date with changes in the primary system. In the case of process equipment, replacement equipment is on hand, or a secondary system is ready and able to perform processing if the first system fails.
- Assets with high confidentiality requirements are encrypted in transport and in storage, and all the necessary technology and management processes are in place to support the solution.
- Assets with high confidentiality requirements are segregated from other data sets, and access control mechanisms are stronger than on systems with lower confidentiality assurance.
- Assets with high assurance requirements get dedicated servers and other dedicated support systems, which are not shared with other assets.
- Assets with high assurance requirements are segregated into their own network environments with strong access controls in place to minimize attack surfaces.
- A high-security assurance configuration standard is created for systems, and this standard is used on all systems which will provide service for assets that have high security requirements.
- Management controls for each environment are already in place to meet the security assurance requirements of those environments.

Once complete, an organization will have in place series of systems and services which apply to different security assurance requirements. Once an asset goes through the impact analysis and security assurance requirements are selected for it, not only will the organization already know which controls to use to secure the asset, an environment will already be created and management processes will already be in place to provide the assurance level required.

4.4.6 Procurement

Most organizations do not include security requirements in their process for choosing products. Many other performance criteria are included in evaluating product for suitability in an organization. Security requirements should also be included.

An excellent document describing how to include security specific language into procurement contracts is the “Cyber Security Procurement Language for Control Systems” document from the US Department of Homeland Security.

4.5 Assessments - Threats, Risks, and Vulnerabilities

In order to understand the security assurance levels and control requirements of assets in your environment, it is important to understand what the risks to your environment are. In order to know your risks, you must assess them periodically.

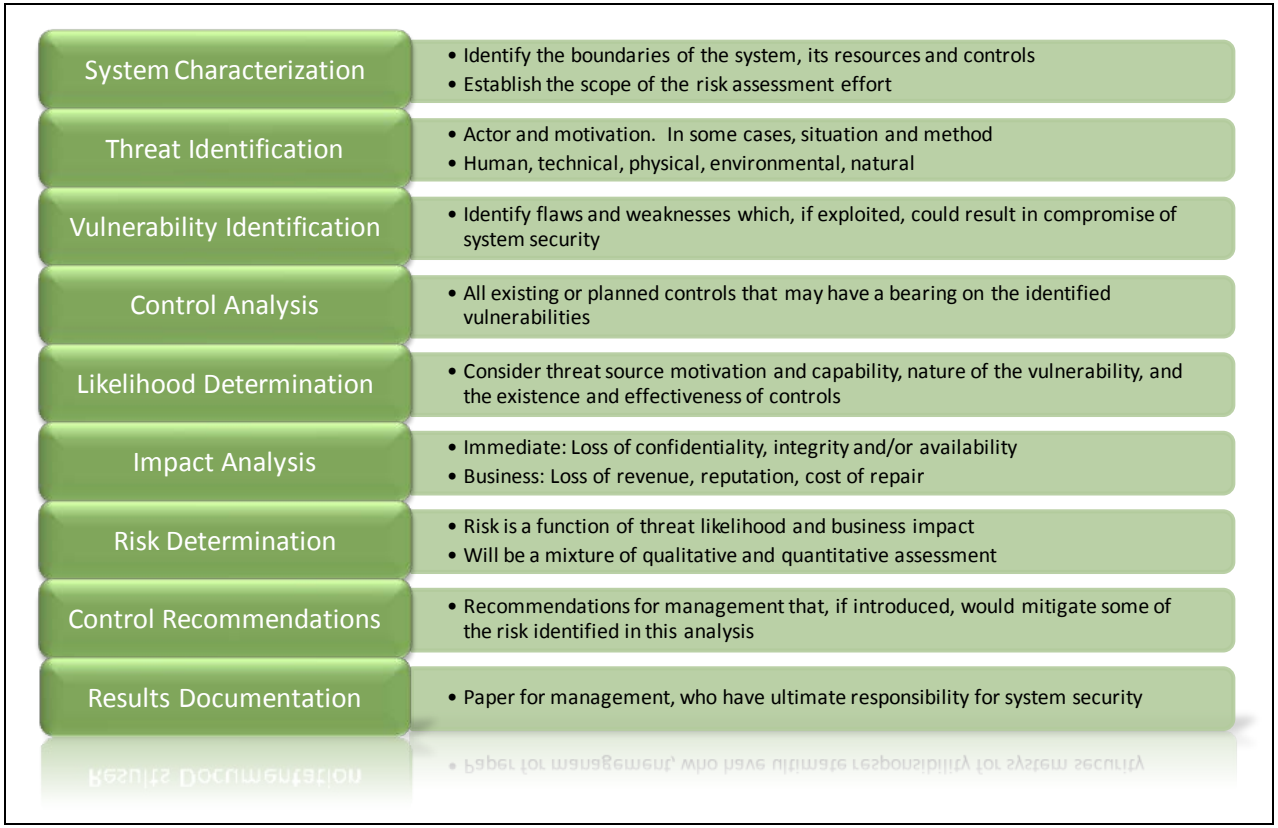
Risk is defined as the product of threat, vulnerability and consequence. R=TVC

Threat – A threat is the possibility of harm of some kind. A threat agent or actor is an individual, group or natural occurrence which can cause undesired consequence either by intentional or unintentional actions. Any threat analysis should, when possible, define the likelihood that a threat agent will attempt to cause a target harm.

Vulnerability – A vulnerability is a security weakness which can be exploited by a threat to cause an undesired consequence in the system.

Consequence – Consequence is the impact to an organization of the exploitation of a vulnerability.

The following diagram illustrates the steps necessary to evaluate threats and risks, and provide control recommendations to remediate those risks.



Threats

Threat agents make threats become reality by exploiting vulnerabilities, and the SCADA/ICS community generally defines three types of threat agent, sorted by their level of threat capability.

Group 1 threat agents are typical hackers and unorganized groups, nuisances, and those actors looking for recognition. These threat agents can attack any target but are seldom motivated to select particular targets. Mostly they are motivated simply to exercise their ability to successfully perform an attack. They look for targets of opportunity, and when faced with systems that are well protected will often move on to easier targets. Group 1 threat agents are not usually particularly sophisticated about their attack methods, and many times will not hide their activities. Nor are

they likely to be asymmetric in their approach. Finally, many Group 1 threats are not usually out to cause significant harm, but may do so as an unintended consequence of their activities.

Group 2 threat agents have a more systematic approach to their activities, and are somewhat well-motivated, usually by the prospect of monetary gains. This threat category includes groups with structure and cause, and often includes agents with similar or common goals. This can include organized crime syndicates, companies engaging in corporate espionage, and 'hacktivisits'. They will be more sophisticated in their approach, using multiple attack techniques in asymmetric ways. For example, instead of only using network and system attack tools to acquire their target, they will employ additional techniques, such as impersonation, bribery, and others. They may be indirect in their approach and add some asymmetry to their attacks. Group 2 threat agents generally do not want to be caught so they will attempt to hide their activities. And while Group 2 threat agents do look for targets of opportunity that can enhance their goals they are not generally opportunistic in their operations. Their objectives are more sophisticated, and they can be more dedicated than those in Group 1.

Group 3 threat agents are highly sophisticated, highly motivated and may have an extended pool of resources to help advance their mission. Those motivations can be political in nature and they are not above causing devastating harm to their targets or even collateral damage if it aligns with their objectives. Typically they are also well funded and/or resourced. Their objectives are broad, complicated, and far reaching so as to include with strategic and tactical elements. Their attack methods will be sophisticated, multi-disciplinary, highly organized, and asymmetrical. It is unlikely that any particular organization or resource will be the sole target of a Group 3 attack – often their targets (and any attacks made on them) are smaller parts in a broader set of targets and objectives. They may 'stack' attacks to hide one within the other, or perform additional attacks which are unrelated to their objectives to confuse anyone who might notice and investigate. Military agencies, state actors, and terrorist groups can contribute to the Group 3 threat actor profiles.

In evaluating any group's capabilities, however, lack of technical ability does not allow a particular group to be dismissed from consideration as a potential threat. Funding is equivalent to resources – a group without expertise can purchase or extort expertise if they have need.

Vulnerabilities

Vulnerabilities are attributes or systems functions that can, under certain conditions, be manipulated in manner to create undesired consequences. Often referred to as 'security weaknesses' vulnerabilities can be created intentionally or unintentionally and provide an opportunity for an attacker or threat to exploit it for gain. They can be introduced by poor manufacturing, poor configuration, incorrect installation, incorrect use, or lack of sufficient management or technical controls.

It is important for an organization to enumerate and understand the vulnerabilities in their systems and processes so that appropriate controls can be put in place to close the gap. Every vulnerability will have an associated risk, and organizational managers must know their risks in order to make informed decisions on how to mitigate those risks or, alternately, accept them. From a SCADA and ICS perspective, this is very important. Study results have shown that in addition to the almost 250 known vendor-specific vulnerabilities, countless security vulnerabilities exists in the commercial operating systems and 3rd part applications used to support SCADA operations. Mitigating these issues, as has been demonstrated in numerous research activities, can non-trivial due to the unique availability requirements of SCADA systems.

In order to be knowledgeable about the vulnerabilities in their environment, an organization must perform periodic vulnerability assessments. There are myriad tools available for free and for hire to accomplish vulnerability assessments, but it is important that the assessment be thorough and exhaustive.

Consequence Analysis

When evaluating possible consequences, we are not examining the threat we are examining the consequence of the threat. Examples include loss of revenue, repair and replacement costs, injury and death, loss of reputation, and others. Some of these look the same as items listed in the threats section. They differ by volume. In threats we did not examine the magnitude of the consequence. So while a threat example might be threat of injury, in consequence analysis we ask what is the likely magnitude of injury – how many people will be hurt and how bad? How much revenue will be lost? What will be the repair and replacement cost? How much will our stock prices dip as a result of loss of reputation?

And in evaluating consequences, we must take into consideration any controls that are already in place. Physical barriers reduce the likelihood that workers will be close to machinery that can injure them. Strong physical access controls limit access to network and system resources. Strong logical access controls limit access to system resources and process control. Controls can reduce or eliminate vulnerabilities, they can limit damage, or they can reduce the threat agent pool. Each will impact the ultimate evaluation of risk.

4.5.1 Risk Acceptance

A concept used sparingly in organizations is that of risk acceptance. Once risks have been identified, an organization can handle them in one of three ways. The first is to eliminate or reduce the risk through additional controls. The second is to transfer the risk by insuring against it. The third is to accept the risk and continue to operate.

Many organizations accept risks regularly. The problem is that often they do so without realizing it. The risk assessment methods discussed above will help managers understand their cyber security risks. And it is an acceptable practice to accept risks and continue operations knowing that they are unresolved. However, they must be formally approved and accepted by a responsible manager ad not simply ignored. They must be revisited periodically to determine whether operating with those risks continues to make sense in the face of updated control technologies and techniques. It is important for business leaders to always know what risks are present in their operations. Without that knowledge they cannot make informed business decisions.

4.6 Personnel Security

4.6.1 Roles and Responsibilities

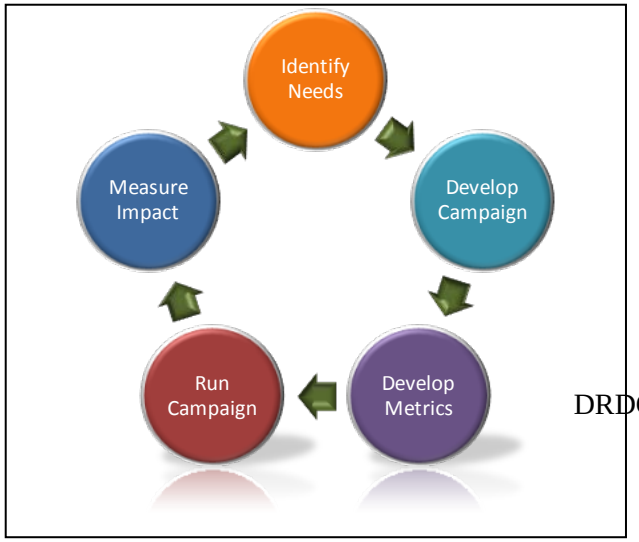
A mature model for any type of information, system, or process management is to push authority and accountability for decisions as close to the asset as possible. Certainly this is a trend in IT and has always been the case in SCADA environments. In SCADA systems, control system engineers are entrusted with the authority they require to manage systems for the benefit of the process they control. Engineers configure systems to tune performance, they respond to incidents, design and deploy new systems for new processes, redesign and deploy devices to better manage existing processes, and recover or replace failing devices. So long as the engineers are the final arbiters for managing control systems they should be provided the training and authority to make certain security related decisions for the devices they manage, within the broader framework of organizational security policy.

This model can, and should, be extended to other ICS staff members. Security operations can be divided up between engineers, operators, and ICS system administrators. This frees security professionals to oversee the process of managing the security program and assessing ongoing compliance with policies and standards while placing security operations management into the hands of operational managers. This management model is more complex than centralized authority and thus requires more effort in several management areas, such as governance, training, change management, and risk assessments. It also runs contrary to many people's notions of traditional hierarchical management. As a result, it takes more time and effort to train managers to work effectively in such a model. For these reasons few organizations adopt it.

4.6.2 Training

Training staff on security issues is a very important part of a security program. In fact, it is likely the single most efficient method for improving overall security of an organization. All staff members need to understand the commitment an organization has made to ICS security and should be regularly reminded of basic security issues that they can put into practice every day.

In addition, particular staff will have need of additional security training. ICS engineers should be familiar with security issues that affect control systems, including emerging malware directed at ICS and vulnerabilities on ICS components. SCADA and support system administrators should be familiar with IT related security issues such as change control, system hardening, patch management, and access control principles as well as ICS vulnerabilities and malware.



4.6.3 Awareness

Awareness is not the same as training. Security specific training does raise awareness but awareness activities are much more subtle. Awareness campaigns for SCADA and ICS domains can resemble marketing campaigns, and use similar techniques. In the past, this approach has proved very successful in the industrial automation domain as it takes into consideration historical cultural and operation nuances traditionally not seen in standard IT environments. Emailing newsletters containing information about security incidents and how they were handled or events that have occurred elsewhere in the world that could impact the organization is one method of increasing awareness through direct communication. When the content is specific to ICS operations, or even relevant to the actual process and business type, this type of communication can be very impactful. Another method is to write articles about specific security issues that affect the individuals and their environment at a level they can digest, such as viruses, memory stick security and other issues that can have a definitive impact on the security profile of a SCADA system.

There are some techniques available that have been proven in the SCADA/ICS domain. Some examples:

- Develop a list of security related incidents within the organization over a 3 month time period, broken down by whichever demographic will be used for targeting groups for awareness campaigns. Perform the campaign, and then measure incidents in that demographic over the same period after the campaign is completed. The difference in incidents before and after the campaign is a measure of its success. This is not a perfect measurement, and will have to be done repeatedly to gain confidence that the change in the frequency of incidents is due to the awareness campaign and not due to other events.

- Take surveys of staff members about incidents, vulnerabilities or security issues that concern them. This can include a discussion about their own environment as well as what they have heard about incidents and vulnerabilities from other sources. This will allow the staff members to feel part of the process and have voice in the process of formulating security policies and procedures. Survey questions have to be formulated carefully so that participants do not feel that they are writing a test, nor should they feel that they are informing on other staff members.

Creativity in the development of metrics is to be encouraged. Over time organizations will be able to tune their metrics to more accurately measure security awareness effectiveness. Implementing a security awareness process will improve general security awareness and promote a more security conscious culture.

4.6.4 Controls

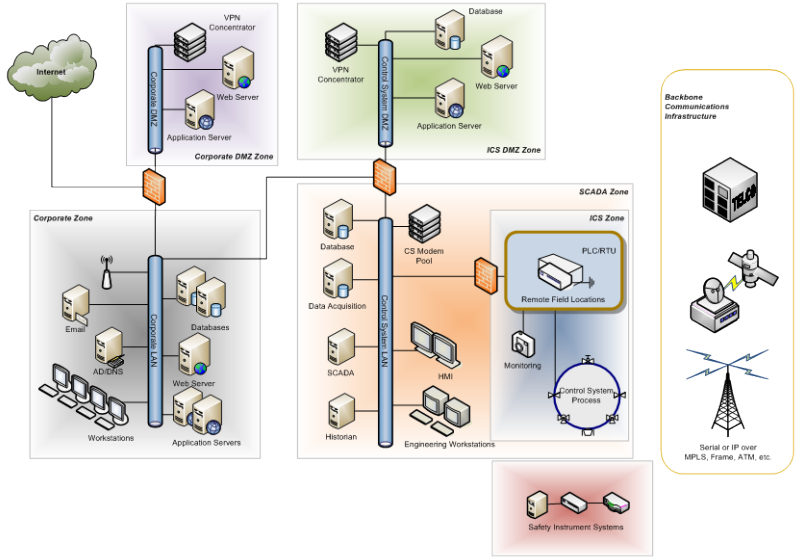
An organization requires a comprehensive catalogue of management, operational, and technical controls from which to select in order to reduce security risks in their environments as they are discovered. Some of the standards mentioned above contain just such lists of controls, with detailed components. The following list shows the NIST 800-53 family of security controls.

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

The table above represents a comprehensive set of controls for information systems which can also be applied to industrial control systems. In the following sections important control concepts are highlighted.

4.6.5 Network Access Control

Networks allow systems to communicate with one another. This allows information sharing, distributed applications, and remote control of other systems. Unfortunately, most systems have vulnerabilities in their systems which are accessible across network communications. Systems have unnecessary services installed and active which are not mission critical, such as web servers, mail servers, ftp servers and others which can have vulnerabilities in them. The systems can have vulnerabilities in their communications packages. Even mission critical services like database servers and application servers, can have exploitable vulnerabilities in them. If all these systems are connected to the same network problems on one system can propagate to other systems. This problem is well known, and IT environments have gone a long way to solving these issues. Firewalls are available to divide networks of systems and devices into zones and restrict the communications between these zones. It is appropriate to place systems with similar security requirements into zones which can then be configured to provide appropriate levels of security assurance to the devices in that zone.



Observe the notional diagram above, and note the placement of firewalls. The SCADA zone, which contains operator stations and operational management software for operators, is separated from the corporate network and its attached Internet to prevent risks from those environments from propagating into the SCADA zone. In order to reduce exposure to risks based on communications from the Corporate zone into the SCADA zone, an ICS DMZ zone was created. Corporate users who need access to ICS data are provided that data out of the ICS DMZ zone, and do not have to connect into the SCADA zone.

Note also that a firewall was erected between the SCADA zone and the ICS zone. The ICS zone contains the field devices and processes being managed by systems in the SCADA zone. This firewall is present to protect the SCADA zone systems from ICS zone systems. This is because the ICS zone could be geographically distributed. In geographically distributed control systems there may be little physical security at those remote locations. If an attacker gains physical access to the network at ICS endpoints they would have access to the SCADA zone systems. A close observer of the diagram might also note that there is a remote access server on the ICS zone. Best practices contraindicate this

configuration. Where possible, remote access devices should be separated from high-security zones, and access into high-security zones managed through firewalls and other access control mechanisms. Compensating controls such as strong authentication and activity monitoring can reduce the risk of allowing remote connections directly into the ICS zone.

4.6.6 System Hardening

ICS systems are 'specific use' systems but the support systems which program them, manage them, and collect data from them are general use systems. As general use systems, support systems are configured for ease of use and maximum utility rather than maximum security. There are extraneous services running on the systems, the services provides are insecure versions of those services, guest users may be enabled, users have more privileges than necessary, applications and services are running with higher privileges than they require. Thus, the security of the system is often poor and does not conform to the principle of least privilege. Guidance includes:

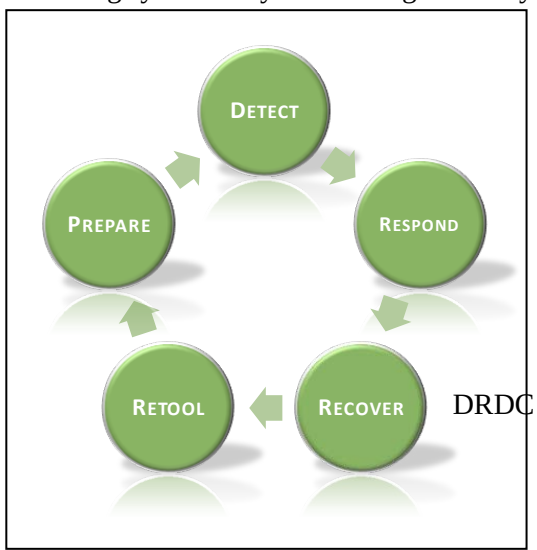
- Unused services and user accounts should be disabled or removed
- Required services should be upgraded to secure versions
- Communications should be configured to be protected encrypted where possible
- User privileges should be reduced to the minimum required to perform their function
- Applications should be run with the minimum privilege necessary

In addition to the above hardening issues, ongoing management of the security posture of the system is required. Vulnerabilities in systems are discovered daily. Security patches need to be installed quickly and efficiently when they are made available by vendors, and done so after testing for compatibility with critical applications running on the system.

An oft neglected system security principle occurs when decommissioning systems. Systems in high-security zones have high-security information on them, whether it is business data or configuration data for high-security ICS devices. When decommissioning or re-tasking systems in an ICS environment the systems should be erased or the non-volatile memory destroyed before redeploying the system for other purposes.

4.6.7 Incident Response

Incident response is the process of detecting and responding to incidents and events which occur on systems and networks. The diagram to the right descibes graphically the incident



response process. The ability to respond to an incident pre-supposes the ability to detect incidents, so robust detective mechansms are required. The controls contained withint the various ICS security standards provide guidance on how to deploy detection mechanisms and collate and examine the data generated.

When an anomalous event is detected the organization must respond. A response plan must be created and implemented which outlines organizational priorities and provides authority to an incident response team to respond to the incident. This also requires that an incident response leader be trained and available to manage the response effort.

Incident response is a complex task that requires interaction with many stakeholders from operations, administration, and management. Beyond possessing the skills and knowledge necessary to manage an incident, an incident response team leader should be experienced with the environments they are investigating, with the people in those environments, and with the stakeholders they have to coordinate with during incident investigation. As part of the incident response priorities, an organization must decide whether it is more important to catch and punish perpetrators or restore services when an incident occurs. Catching and prosecuting perpetrators involves law enforcement and the courts, which in turn requires certain strict procedures on investigating the incident and collecting and preserving evidence.But whether or not prosecution is a priority, system operators, engineers and administrators need to be trained how to handle systems when they suspect an incident has occurred so that their reactions do not needlessly erase important information needed to support an investigation.

4.7 Conclusions

Systems security management programs, as a concept, are not limited to IT environments. The security management program is a process which evaluates risks and selects controls to mitigate those risks. As a process, it can incorporate the special requirements of ICS environments and thus can be used to manage the security risks in ICS.

Currently, the volume of best practice security guidance available to SCADA and ICS asset owners is extensive. The ubiquity of security issues across the Canadian asset owner landscape allows for these practices to be applied across many sectors, while simultaneously addressing some of the unique challenges facing Canadian stakeholders. This study was able to assess the current state of available guidance and extract high-level direction that the Canadian asset owners can use to create effective SCADA resilience plans. This approach was discussed by study partners, and rather than simply re-create existing guidance in a new format it was deemed more useful to prove insight to key overarching themes and supply a concise, well-researched set of references.

Based on the reviews of available best practiced and standards, combined with real-work experience demonstrated by the study team, the following high-level guidance can be provided to the Canadian community of interest. This guidance is to be considered complimentary to the granular direction provided in exiting literature and practices.

1. Assign a senior manager to be responsible for managing cyber security risks in ICS environments, and cross pollinate personnel between IT and SCADA on a regular basis.

2. Create a Security Management Program to assess and remediate risks with appropriate controls, accept residual risks, manage incidents, measure program success and perform self-improvement.

3. Identify every asset in the ICS environment and assign criticality to it. Establish its security assurance requirements based on an impact analysis, and use these results to shape processes for incident investigation and forensic activity.

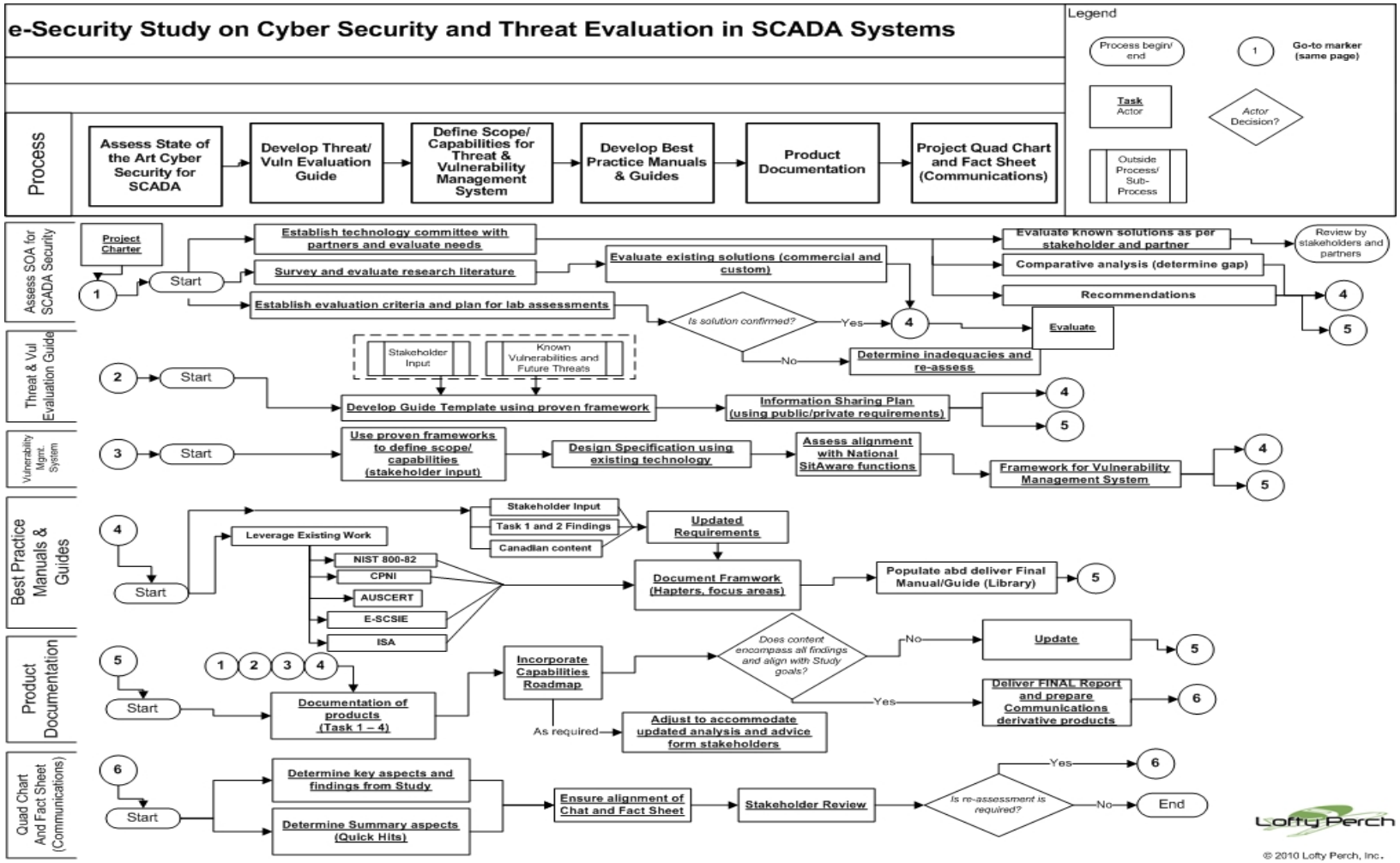
4. Ensure a strong change management program is in place to reduce the risk that unauthorized or undocumented changes can occur to systems, applications and networks.

5. Create a comprehensive set of controls which match with security assurance (and system criticality requirements. Consider adopting a standard, if one is not already mandated by regulatory requirements, and make appropriate modifications to fit your environment.

    - Group systems with similar security requirements into access controlled network environments.
    - Ensure proper change management practices are observed so that administrators can be confident that they are aware of the state of the environment, including the state of security.
    - Provide dedicated systems for critical services and applications.
    - Harden systems and applications by removing extraneous functionality, improving authentication mechanisms, and improving access control enforcement, in accordance with the principle of least privilege.

6. Implement a robust incident management program, with resolution deadlines and the ability to evaluate and improve itself. This program should include robust anomaly detection mechanisms across environments, systems and applications.

Annex M Project workflow



Annex N References

Cyber Security Policy Planning and Preparation

- TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004.
- NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Final Public Draft September 29, 2008.
- NIST SP 800-53 Rev 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.
- Additional Information
- "21 Steps to Improve Cyber Security of SCADA Networks," Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, U.S. Department of Energy.
- Kilman, D. and Stamp, J. "Framework for SCADA Security Policy," Sandia Corporation. 2005.
- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program.
- NIST SP 800-64 Revision 2, Security Considerations in the System Development Life Cycle, October 2008

DMZs and Network Segmentation

- Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, Centre for the Protection of National Infrastructure (CPNI), London, 2005 - *http://www.oe.energy.gov/DocumentsandMedia/Firewall_Deployment.pdf*
- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook - *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*
- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program - *http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf*
- Control Systems Cyber Security: Defense in Depth Strategies, May 2009, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program. - http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

Patch and Configuration Management

- NIST SP: 800-40, Creating a Patch and Vulnerability Management Program, 2005 - *http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf*
- NIST SP: 800-118, Guide to Enterprise Password Management (Draft), - *http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf*
- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook - *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*

ICS Specific Security Training

- Wilson, Mark, Hash, Joan, NIST SP: 800-50, Building an Information Technology Security Awareness and Training Program, 2003 - *http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf*

Risk and Vulnerability Assessments

- Rinaldi, et al, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, 2001 - *http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf*

- GAO-04-354, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, U.S. GAO, 2004 - *http://www.gao.gov/new.items/d04354.pdf*
- Stamp, Jason, et al., Common Vulnerabilities in Critical Infrastructure Control Systems, Sandia National Laboratories, 2003 - *http://www.sandia.gov/scada/documents/031172C.pdf*
- Duggan, David, et al, Penetration Testing of Industrial Control Systems, Sandia National Laboratories, Report No SAND2005-2846P, 2005 - *http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf*
- NIST SP: 800-34 Rev. 1, Contingency Planning Guide for Information Technology Systems, 2010 - *http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf*
- NIST SP: 800-61 Rev. 1, Computer Security Incident Handling Guide, March 2008 - *http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf*
- NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008 - *http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf*
- NIST SP: 800-115, Technical Guide to Information Security Testing and Assessment, September 2008 - *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*

ICS Security Procurement Requirements

- SCADA and Control Systems Procurement Language Project. - *http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf*
- Security Technologies for Industrial Automation and Control Systems -- *http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9665*
- Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004 - *http://www.isa.org/Template.cfm?Section=books&template=Ecommerce/FileDisplay.cfm&ProductID=7380&file=Preview.pdf*

IDS/IPS Usage and Placement

- NIST SP: 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) - *http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf*
- Wooldridge, S. "SCADA/Business Network Separation: Securing an Integrated System," 2005. http://www.automation.com/sitepages/pid1363.php
- Ashier, J. and Weiss, J. "Securing your Control System," 2004. - *http://www.controlglobal.com/articles/2004/238.html*
- Network Monitoring System Designed to Detect Unwanted Wireless Networks, September 14, 2005 - *http://www.controlglobal.com/industrynews/2005/168.html*
- Rakaczky, E. "Intrusion Insights Best Practices for Control System Security," July 2005 - *http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=45286*
- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program – *http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf*
- Control Systems Cyber Security: Defense in Depth Strategies, May 2006, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program. – *http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf*
- Mitigations for Security Vulnerabilities Found in Control System Networks, June 2006, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program - *http://www.us-cert.gov/control_systems/practices/documents/MitigationsForVulnerabilitiesCSNetsISA.pdf*

Authentication, Authorization, and Access Control For Direct and Remote Connectivity

- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook. - *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*

- NIST SP: 800-73-2, Interfaces for Personal Identity Verification (4 parts), September 2008. *http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf*
- NIST SP 800-76-1, Biometric Data Specification for Personal Identity Verification, 2007. - *http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf*
- Baker, Elaine, et al, NIST SP: 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007. - *http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf*
- NIST SP 800-53 Rev 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009. *http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf*
- NIST SP: 800-57 Recommendation for Key Management, March 2007
    1. Part 1, General (Revised) *http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf*
    2. Part 2, Best Practices *http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf*
    3. Part 3, Application Specific Key Management Guidance (Draft), October 2008 *http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf*
- NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Final Public Draft September 29, 2008. - *http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*
- Wooldridge, S. "SCADA/Business Network Separation: Securing an Integrated System," 2005. *http://www.automation.com/sitepages/pid1363.php*
- Ashier, J. and Weiss, J. "Securing your Control System," http://www.controlglobal.com/articles/2004/238.html2004. *http://www.controlglobal.com/articles/2004/238.html*
- "Thales e-Security." 2005. *http://www.controlglobal.com/vendors/products/2005/207.html*
- Schwaiger, C. and Treytl, A. "Smart Card Based Security for Fieldbus Systems," 2003, Austria Card, Vienna, Austria. *http://www.ict.tuwien.ac.at/staff/treytl/papers/etfa03_teaser.pdf*
- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program. *http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf*

Securing Wireless Connections

- NIST SP: 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008. *http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf*
- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
- Pescatore, J. "Keep your Wireless Business Secure," August 21, 2005. *http://www.controlglobal.com/articles/2005/476.html*
- Network Monitoring System Designed to Detect Unwanted Wireless Networks, September 14, 2005. *http://www.controlglobal.com/industrynews/2005/168.html*
- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program. *http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf*
- Securing ZigBee Wireless Networks in Process Control System Environment (draft), April 2007, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program - *http://www.us-cert.gov/control_systems/practices/documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf*

Use of VPNs and Encryption in Securing Communications

- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook. - *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*
- NIST SP: 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007. *http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf*
- SP 800-56 B, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, August 2009 -
- NIST SP: 800-57 Recommendation for Key Management, March 2007
    1. Part 1, General (Revised) *http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf*
    2. Part 2, Best Practices *http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf*
    3. Part 3, Application Specific Key Management Guidance (Draft), October 2008 *http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf*
- AGA Report No. 12: Cryptographic Protection of SCADA Communications Part 1 Background Policies and Test Plan, American Gas Association, 2006. *http://www.aga.org/our-issues/security/Documents/0603REPORT12.PDF*
- Peterson, D. "Protocol for SCADA Field Communications," July 12, 2005. *http://www.controlglobal.com/articles/2005/424.html*
- Cohen, B. "VPN Gateway Appliances-Access Remote Data like the Big Guys," April 28, 2005. *http://www.smallbusinesscomputing.com/testdrive/article.php/3501156*
- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program. *http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf*

Establishing a Secure Topology and Architecture

- NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook. *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*
- NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Final Public Draft, *September 29, 2008. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*
- "Study Suggest Increased Concerns with Cyber Security and SCADA System Reliability," June 14, 2005. *http://www.controlglobal.com/industrynews/2005/131.html*
- Berg, M. and Stamp, J. "A Reference Model for Control and Automation Systems in Electric Power," Sandia Corporation. 2005. *http://www.sandia.gov/scada/documents/sand_2005_1000C.pdf*
- Control Systems Cyber Security: Defense in Depth Strategies, October 2009, U.S. Department of Homeland Security National Cyber Security Division, Control Systems Security Program. *http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf*
- Curtis, Ian, ABB. "Security against cyber attack," July 19, 2010. *http://www.manufacturingchemist.com/technical/article_page/Security_against_cyber_attack/55597*
- Invensys Operations Management (Australia) Pty Ltd. "Integrating control and safety -- where to draw the line," Jan 20, 2009. *http://www.processonline.com.au/articles/32239-Integrating-control-and-safety-where-to-draw-the-line*

Applying and Complying with Security Standards

- TSA Pipeline Security Guidelines, Transportation Security Administration, April 2011. - http://www.aga.org/our-issues/security/Documents/TSA%20Pipeline%20Security%20Guidelines%20-%20Apr%202011.pdf

- INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry, Interstate Natural Gas Association of America (INGAA), April 2011. - *http://www.aga.org/our-issues/security/Documents/INGAAControlSysCyberSecGuidelinesREV.pdf*
- TR99.00.01: Security Technologies for Manufacturing and Control Systems, ISA, 2004. - *http://www.isa.org/isatr9900012007*
- TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004. - *http://www.isa.org/Template.cfm?Section=books&template=Ecommerce/FileDisplay.cfm&ProductID=7380&file=Preview.pdf*
- Peterson, D. and Howard, D. "Cyber Security for the Electric Sector," September 12, 2005. - *http://www.controlglobal.com/articles/2005/477.html*
- Berg, M. and Stamp, J. "A Reference Model for Control and Automation Systems in Electric Power," Sandia Corporation. 2005. *http://www.sandia.gov/scada/documents/sand_2005_1000C.pdf*

Ensuring Security when Modernizing and Upgrading

- TR99.00.01: Security Technologies for Manufacturing and Control Systems, ISA, 2004. - *http://www.isa.org/isatr9900012007*
- Cyber Security Procurement Language for Control Systems, U.S. Department of Homeland Security National Cyber Security Division, September 2009. - *http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf*
- Ladd, E. "Dispelling the myths of HART-enabled devices," April 18, 2005. *http://www.controlglobal.com/articles/2005/368.html*
- Verhappen, I. "What makes a fieldbus go?" April 27, 2005. *http://www.controlglobal.com/articles/2005/209.html*
- Verhappen, I., "On the bus: Design hurdles to fieldbus technology," Control Global, 2005. *http://www.controlglobal.com/articles/2005/385.html*
- NIST SP 800-64 Revision 2, Security Considerations in the System Development Life Cycle, October 2008 *http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf*
- "Supervisory Control and Data Acquisition (SCADA)," Data Comm. for Business, Inc., Oct 1999. *http://www.dcbnet.com/notes/9905scada.html*
- Digital Bond, British Columbia Institute of Technology, and Byres Research. "OPC Security White Paper #1: Understanding OPC and How it is Deployed," July 27, 2007. *http://www.us-cert.gov/control_systems/practices/documents/OPC%20Security%20WP1.pdf*
- Digital Bond, British Columbia Institute of Technology, and Byres Research. "OPC Security White Paper #2: OPC Exposed," November 13, 2007. *http://www.us-cert.gov/control_systems/practices/documents/OPC%20Security%20WP2pdf*
- Digital Bond, British Columbia Institute of Technology, and Byres Research. "OPC Security White Paper #3: Hardening Guidelines for OPC Hosts," November 13, 2007. - *http://www.us-cert.gov/control_systems/practices/documents/OPC%20Security%20WP.pdf*

DHS CSSP Recommended Practices.

- Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies - *http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf*
- Creating Cyber Forensics Plans for Control Systems - *http://www.us-cert.gov/control_systems/practices/documents/Forensics_RP.pdf*
- Developing an Industrial Control Systems Cybersecurity Incident Response Capability - *http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf*
- Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks - *http://www.oe.energy.gov/DocumentsandMedia/Firewall_Deployment.pdf*
- Hardening Guidelines for OPC Hosts - *http://www.us-cert.gov/control_systems/practices/documents/OPC%20Security%20WP3.pdf*

- Mitigations for Security Vulnerabilities Found in Control System Networks - *http://www.us-cert.gov/control_systems/practices/documents/MitigationsForVulnerabilitiesCSNetsISA.pdf*
- Patch Management of Control Systems - *http://www.us-cert.gov/control_systems/practices/documents/PatchManagementRecommendedPractice_Final.pdf*
- Securing Control System Modems - *http://www.us-cert.gov/control_systems/practices/documents/SecuringModems.pdf*
- Securing WLANs Using 802.11i (draft) - *http://www.us-cert.gov/control_systems/practices/documents/Wireless%20802.11i%20Rec%20Practice.pdf*
- Securing ZigBee Wireless Networks in Process Control System Environments (draft) - *http://www.us-cert.gov/control_systems/practices/documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf*
- Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments (draft) - *http://www.us-cert.gov/control_systems/practices/documents/OpSec%20Rec%20Practice.pdf*

5 Introduction Final Study Report, Capability Road Map,Final Quad Chart, and Project Fact Sheet

This document provides a report on specific tasking as it pertains to the 'Final Study Report, Capability Roadmap, Final Quad Chart and Project Fact Sheet'. This document provides material summarizing content developed from a comprehensive review of the reporting across all study tasks. It includes other project completion activities including strategic advisory guidance, capability roadmap, a project fact sheet and a final quad chart for review purposes.

Overall, the study was completed on time and met or exceeded all expectations as defined by study objectives. In addition, due to the experience of the study leadership and their access to technology and industry stakeholders, the study was completed under budget. As the study was performed concurrent with many real-world SCADA security projects being performed by the study research team, additional observations and findings were able to enhance the work done in a laboratory environment.

The study results and recommendations were as follows:

- PSTP study programs that include dedicated activities towards a better understanding of SCADA and control system cyber security have tremendous value to Canadian critical infrastructure asset owners
- The SCADA security technical capabilities and subject matter expertise within the Canadian community of interest is considerable, the current level of interest demonstrated by the federal government is well-positioned to accommodate current and future requirements to leverage this expertise in infrastructure resiliency programs
- Existing commercial security technologies have applicability in SCADA security programs, and those technologies addressing intrusion detection/prevention and forensics can clearly improve defensive strategies when deployed with due care. In many cases, the somewhat standard network configurations of SCADA networks creates opportunities for straightforward defensive strategies applicable across many sectors, and modifications in traditional deployment configurations can greatly improve the protection of control system domains.
- The volume of SCADA security research and information that is available from the global community is substantial, and the ubiquitous problem of how to secure control systems allows this information to have widespread and significant positive impact on the security risk profiles of Canadian critical infrastructure.
- Existing frameworks used by public and private sector entities to manage cyber threats and vulnerabilities are well-suited to accommodate for the requirements associated with SCADA systems. In addition, elements derived from historical approaches to threat and vulnerability management can be updated to create the capabilities to meet future states of threat management requirements.
- The effective deployment of security countermeasures within industrial control system environments is often dependent upon asset owner's willingness and technical expertise to customize commercial security technologies. However, those stakeholders that have created SCADA security risk reduction programs can provide insight that enhances current resiliency strategies and may be better prepared for information sharing with law enforcement and intelligence entities.

- The number of vulnerabilities that are specific to SCADA vendor technology is increasing, as is the understanding of research strategies and the inclusion of these vulnerabilities into contemporary exploit frameworks. In addition, the security of SCADA systems is also significantly impacted by vulnerabilities that are unique to underlying operating systems or third-party applications (as opposed to specific SCADA vendor solutions).

- The number of standards and recommended practices specific to SCADA security has increased considerably in the recent year, as has the amount of usable guidance uniquely designed for individual critical infrastructure sectors

As previous work has been delivered to the project technical authority this document has been designed for brevity and is concise in structure. Supporting material for this document is contained in previously delivered information products, in this document is designed to provide an overall summary of project study findings.

5.1 Study activities and observations

Task 1 – Assess the State of the Art for SCADA Security
The tasking in this project area was comprised of three core activities, all of which were performed with the study's primary and supporting objectives in mind:
Evaluate existing security technologies in view of identifying the best solutions for capturing wired and wireless SCADA traffic and detecting malicious activity.

Identify the capability gaps in efficiently detecting malicious traffic targeting SCADA systems, and survey and evaluate the research literature in relation to work being done to improve this capability.

Evaluate forensic technologies and techniques that can be leveraged to understand the response of SCADA systems to malicious traffic.

Lofty Perch, Inc. (LPI) and the study team performed extensive research during this study activity, and in addition to working on other study areas concurrently, LPI executed lab and field based testing in collaboration with industry stakeholders and in-kind partners. LPI made significant findings regarding communications capture techniques in SCADA and control system domains, and cross-correlated their findings with study work on intrusion detection and intrusion prevention capabilities. Perhaps most interesting is the fact that during the actual work activities LPI was involved in two (2) cyber-security incidents and seven (7) security assessments involving industrial control systems. Using their on-site experience, the study team was able to make significant contributions to the study's requirements involving the evaluation of security technologies and techniques applicable to SCADA and industrial automation. The integration of findings from the resultant field work allowed for direct investigation pertinent to specific study tasking areas while actively supporting the study's primary and complementary objectives.

The sub-tasking for the evaluation of existing security technologies that capture wired and wireless traffic to detect malicious activity on a control system network indicates that current commercial-off-the-shelf (COTS) and open-source network analysis tools are adequate for performing traffic analysis. However,

current technology is best suited for network based communications, and there are a number of technical capability requirements that vary depending on the complexity of the architecture. Although existing traffic analysis technologies are suitable for non-routed protocols, the study has shown that the most effective capabilities exist when analysis is being performed in a networking environment.

The detection of malicious traffic is dependent on tuning the technology to either look for deviations in normal communications behaviour or to incorporate known intrusion signatures into the analysis. The study shows that technology designed to detect malicious traffic, or more accurately technology that can be tuned for SCADA environments, can only be optimized fully when administered by a subject matter expert. To that end, the subject matter expertise required to optimize malicious traffic detection capabilities should be specific to the control system domain and, perhaps more importantly, specific to the actual control system technology and communication protocol. This observation suggests that future strategies for defending against malicious activity in SCADA networks will an active collaboration between the IT security, engineering, and vendor domains.

The study team performed a comprehensive review of existing literature regarding historical perspectives on the functional requirements for detecting and mitigating abnormal and possibly malicious traffic targeting SCADA systems. During this review, a contrast and compare of historical and current/future trending was performed, and it was observed that a significant amount of academic and independent research provides a foundation for future technology development. It was also noted that several government research and development projects have resulted in technology specific for traffic analysis and intrusion detection for control systems, and that some of this technology is being transferred into the private sector domain. The rate at which this technology is being developed and deployed is concurrent with the growing security needs asset owners are experiencing. From this, it may be concluded that the gap between contemporary intrusion detection requirements and intrusion detection requirements for SCADA systems is closing, but more work is required.

This initial task also focused on the evaluation of forensic technologies and techniques that can be used in responding to SCADA system security events and analyzing malicious traffic. As mentioned above, during the study period the research team was engaged in two incident response engagements that directly involved the application of contemporary forensic investigation techniques and technologies, while simultaneously supporting investigations using current best practices and guidance. The observations and analysis from this activity has resulted in an improved understanding of current forensic computing approaches as applied to SCADA systems, and has uncovered some existing gaps in both techniques and technologies required to perform comprehensive investigations on industrial automation.
Concurrent to these field investigations, the study team worked closely with in-kind partners to perform analysis of commercial forensic technologies and determine if and how they can accommodate the unique operational environments associated with SCADA systems. This activity also coincided with regular interactions with several national law enforcement and intelligence entities, resulting in a substantial set of conclusions that have proven useful in other study task areas.
The tasking performed during the study period aligned with project expectations, timelines, and the planned workflow. Research and analysis performed in both laboratory and real-world environments demonstrated that contemporary security technologies designed for traffic analysis and forensics show good promise in supporting cyber-security activities in SCADA system environments. The study was able to determine gaps in existing technologies, and define what future solutions require to meet the unique demands of industrial control system environments. The information derived from the analysis provided content for the creation of a capabilities matrix that stakeholders can use in analyzing a broad scope of different control system architectures.
As expected, the issues related to the effectiveness of traffic analysis and forensic technologies do not lie solely in the technological capabilities themselves. The study showed that the current state-of-the-art in cyber-security does indeed provide effective capabilities for protecting SCADA systems but the

effectiveness of those solutions is highly dependent on the subject matter expertise and engineering capability needed to configure, deploy, and manage them. In addition to determining what gaps exist in current technologies the report provides insight to a set of well-defined methodologies and approaches that can ensure the usefulness of the technologies is maximized for use on SCADA systems.
The information in this report has been developed to accommodate for the requirements as cited in the study tasking. This deliverable is intended to provide a foundation for subsequent study tasking addressing issues of threat and vulnerability evaluation guides, cyber-threat matrices, an analysis of existing and future SCADA vulnerabilities, and plausible requirements for a cyber-threat and vulnerability management system. The research results obtained in this initial Task 1, in combination with the results from study Task 2, were be used to support the development of a Best Practices Security Manual or Guide for Canada's critical infrastructure owners and operators.
A comprehensive set of deliverables was presented during the lifecycle of the project, and in the interest of brevity the content in this final report does not go into the granular depth that specific task deliverables do.

Task 2 – Development of a Cyber-Threat and Vulnerability Evaluation Guide
The tasking in this project area was comprised of three core activities, all of which were performed with the study's primary and supporting objectives in mind:
Define a cyber-threat matrix in consultation with critical infrastructure owners or operators, law enforcement, and the intelligence community.

Perform a review of the known vulnerabilities of SCADA systems, and project future threats and vulnerabilities to provide direction to future research areas.

Identify various approaches to address the privacy concerns of private sector owners or operators in view of sharing cyber-threat and vulnerability reports with the Community of Practice (CoP) and the federal government.

Lofty Perch, Inc. (LPI) and the study team performed extensive research during this study activity, and in addition to collaborating with industry stakeholders participated in numerous seminars and symposia dedicated to understanding the cyber threat landscape as it pertains to SCADA. Understanding that the tasking would result in material to provide for a cyber-threat and vulnerability evaluation guide, activities were performed concurrently to ensure that the materials accounted for vulnerabilities in control systems as well as take into consideration threats from the perspective of the stakeholder community. The report showed that the perceived categories of cyber threat, from the stakeholder community, may have significant impact on critical infrastructure protection and resiliency.

The report showed that the perspectives on cyber-threat to SCADA systems differ between the stakeholder, law enforcement, and intelligence (i.e. national security) communities. As such, the components of the report attempts to close this knowledge gap and takes into consideration that public sector entities have a significant reliance on information from the private sector community. This theme was consistent across all communities of interest engaged for the project, and illustrates how the law enforcement and intelligence communities may be at a disadvantage in terms of collecting information for protecting national critical infrastructure assets from cyber-threats. The study also revealed that asset owners are not convinced that the level of technical capability maintained by the law enforcement or intelligence community is appropriate to fully understand cyber-threat and consequence to critical infrastructure operations, and this may result in a lack of reporting to authorities.

The study indicated that some progress has been made in the establishment of various approaches to address the privacy concerns of private sector asset owners with regards to sharing cyber-threat information, but the existing frameworks may require enhancement. The report showed that not all contemporary solutions for information sharing involve the federal government, but rather it is the growing presence of independent research and academic institutions that are providing portals for asset owners to share vulnerability and incident reporting. Impediments to information sharing are slowly being recognized, but new approaches are required to create public/private collaboration mechanisms. The study was able to demonstrate that effective mechanisms for trusted collaboration are emerging, and as these agreements mature they may mitigate many of the concerns shared across the private sector asset owner community. The report demonstrated that a significant portion of the stakeholder community remains unwilling to share cyber-threat and vulnerability data with the public sector, even though useful Memorandums of Understanding (MoU's) have potential in helping facilitate intelligence sharing.

It was anticipated that the activities in this study task would present difficulties insofar as obtaining detailed threat information from the federal law enforcement and intelligence communities. This concern was realized, possibly due to the absence of technical expertise within many of the stakeholder environments. However, the study team was able to leverage its extensive network of relationships to mitigate this problem and extract detailed information from the asset owner community (and thus obtain insight from those entities dealing with cyber-threat on a day-to-day basis). Access to various Canadian law enforcement and intelligence entities was limited during the course of the tasking, and as such the study team executed tasking activities in collaboration with law enforcement and intelligence entities with other representatives from the intelligence community.

The results collected from interactions with the stakeholder community regarding perceived threats were surprising, as some domains of interest have not traditionally been considered within the scope of control system/industrial automation. Perhaps the most interesting result was that the study suggests that the asset owner community appears to be predominately concerned with consequences and overall impact of a cyber-event. This is contradictory to the theory that they are primarily concerned about specific threats. The study suggests that the asset owner community is very concerned about the kinetic impact a cyber-incident can have on industrial automation and is less concerned with the threat or adversary (beyond the risk associated with the ever present insider). The stakeholder community feels that a solid understanding of technical vulnerabilities, combined with detailed knowledge about impact when those vulnerabilities are exploited, provides a much clearer approach to proactive and reactive cyber-security strategies. This finding made the development of the evaluation guide elements interesting, as the characteristics associated with threat, and the level of effort to understand them, were very different between private sector asset owners and public sector law enforcement/intelligence agencies.

The study team selected to use a customized version of the CSEC/RCMP Threat Risk Assessment methodology as a foundational framework for the development of the guide. By using this approach, the deliverable would be aligned with the expectations of both the private and public sector communities of interest. This strategic decision may help facilitate for the development of the initial scope and capabilities of a cyber-threat and vulnerability management system for SCADA systems (Task 3), specifically with the possibility of feeding into a national cyber situational awareness capability.

The report provided an opportunity to perform an exhaustive review of the known vulnerabilities specific to industrial control systems. To add more value to the report, the study team also reviewed categories of vulnerabilities that are not control system specific but could ultimately impact control system security. The study analyzed roughly 240 known vulnerabilities specific to industrial automation, approximately 35 non-public vulnerabilities found by the study team, and more than 250 non-SCADA specific vulnerabilities that could impact the security of a control system. It was from this analysis the study team was able to extract a set of plausible future vulnerabilities that could directly impact SCADA security and

derive some characteristics of the future threats exploiting those vulnerabilities. Taking into consideration other project tasking, the study team was able to define several strategic areas that could be used to focus future research. The analysis demonstrated the majority of known vulnerabilities that are specific to industrial control systems impact the system 'availability' attribute. It is generally agreed upon that confidentiality is the most critical security requirement in IT systems, followed by integrity and availability (in that order). Contrary to this, availability is the most critical security requirement in the SCADA and control system domain. This primary requirement is followed by integrity and confidentiality. Research has shown that this perspective is accurate as critical infrastructure systems have extensive availability requirements followed closely by the requirement for sound operational data (integrity). As such, if availability is a primary requirement from a control system security perspective then the fact that a majority of the known vulnerabilities impact system availability is concerning

The information collected during this study task showcased that the concerns regarding cyber-threat to SCADA systems are common across the stakeholder community, with deviations in those concerns being attributable to the nuances associated with sector specific architectures. Fortunately, the scope of this task activity was limited to cyber threats and vulnerabilities, thus allowing for the findings to be interpreted by the reader and applied to their architecture as required. The amount of information collected from open source materials was extensive, and when cross correlated with the input from the stakeholder community the study team was able to craft a solid framework to empower any asset owners in creating a customized threat and vulnerability guide.

The resulting evaluation guide was designed to assess threats, vulnerabilities and risks. After an assessment based on the guide has been completed and the residual risks have been identified in the private sector, stakeholder concerns about *threats* and *threat agents* may be shared with the federal government for management and mitigation, particularly without the implications of fault or vulnerability. A possible approach would be to promote a risk evaluation guide to stakeholders with the offer of assistance in regard to mitigating specific threats once they have determined the risks for themselves.

A key message is to differentiate vulnerability from threats and risks. As an approach to greater engagement between government and asset owners and operators, stakeholders must be educated about the difference between technical vulnerabilities and threats so that the asset owners and operators may be able to provide more precise information about security threats and risks, without incurring business-cost risk from courting regulatory scrutiny of perceived deficiencies.

The focus on technical vulnerability provides "low hanging fruit" for producing new security intelligence since the information is verifiable, and presents fewer challenges to relationships with parties who may object to being classified as a "threat" or a source of risk. However, the technical vulnerability landscape changes daily, sometimes hourly, with the publication and refinement of vulnerability information evolving mostly from collaborative "crowd sourced" efforts on the internet. The collection and development of information about technical vulnerabilities is a class of problem suited to task-specific organizations that can retain the dynamic specialist expertise for point in time analysis, and which can limit their accountabilities to task-based deliverables, all without the overhead of maintaining complex relationships with governments, civil society and interest groups, media and other parties.

For most asset owners and operators, technical vulnerability information about their infrastructure and operations is considered sensitive and it was not clear from interactions with them what benefits compensate them for costs and risks from collecting or producing and disclosing the information.

In engaging private stakeholders, public sector agencies might de-emphasize the focus on individual areas of technical vulnerability in private sector stakeholder systems and operations, which are interpreted (accurately or not) as faults in the organization and in turn expose the organization to risk from being made an example of via regulatory, political or legal intervention. A better understanding of the risks from disclosing technical vulnerability information to a specific government department is required before a persuasive case for disclosing it can be made. Since disclosures are at this point hypothetical, it is

not known how the information might be used, how it would be protected, and again, how or if, providers would be compensated for the resources required to collect it. A plan that supports a broader critical infrastructure security strategy to accomplish national security objectives would provide a foundation for stakeholder engagement from the asset owner and operator community, which would in turn enable the derivation of clear information requirements. These requirements should drive the adoption of practices for information sharing, since without requirements, it is difficult to evaluate the quality and effectiveness of any effort made toward their implementation.

Task 3 – Scope and Capabilities of a Cyber Threat and Vulnerability Management System for SCADA
The tasking in this project area was comprised of several activities, all of which assisted in developing aspects of a future-state cyber-situational awareness capability (bearing in mind that it may feed into a national cyber-situational awareness capability). The tasking was performed to align with proposed activities, and included:
Assess existing and proven management system frameworks and define requirements through collected stakeholder input

Design specifications using (where possible) existing technology

Assess alignment with any known Situational Awareness functions

During the study, it was not possible to ascertain the definitive characteristics of any such management system as it exists is in Canada, however the information collected from stakeholder collaboration efforts and other national capabilities resulted in some good results. In absence of any obvious national-level capability for SCADA, as well as not having access to the government representation able to accurately define current or planned threat and vulnerability management systems, the study team expanded their review of existing private/public sector sharing initiatives (focused on SCADA). The study team correlated findings from existing situational awareness capabilities (non-Canadian) and extracted common themes that could be used to support a cyber-threat/management system for Canadian critical industrial control systems assets and activities.

The study team selected common activities associated with ‘focused national actions’, and developed a framework to allow stakeholders to contribute to which information feeds and sharing forums would support such a capability. The study showed that effective threat and vulnerability management systems are not dedicated solely to understanding the threats and vulnerabilities themselves, but rather they support how information can be used to provide for a proactive (protection) and reactive (recovery) lifecycle. In addition, the study showed that the best approach for a SCADA cyber threat and vulnerability management system incorporates features and characteristics of past management frameworks, and that certain aspects of traditional management frameworks can work well in future-state strategies.
As information sharing was determined to be a critical part of the systems success, the study team revisited the existing frameworks for public/private information sharing. Using findings from previous project study activities, it was determined that existing information sharing frameworks are adequate to facilitate public/private sharing. The study did address high-level activities that government could implement to support the management system. The study team was able to leverage their experience in supporting similar programs around the world, and looked specifically at those projects involving the management of national cyber situational awareness activities as they pertain to SCADA.
One of the more interesting challenges of the tasking was determining what the technology landscape for such a management system would look like. To address this issue, the study team interacted with private and public sector partners that had either fully developed or were it the process of developing a vulnerability/threat management system that could accommodate SCADA datasets. The study shows that a common approach was to use ‘activity’ states to define what the management system is doing and how it supports proactive (steady state) or reactive (response) actions. This, in turn, helped the study team

review a set of applicable operational components and the corresponding partners that would be required to ensure the management system remains effective.

Using an approach that would ensure alignment with Canadian interests (should one exist or evolve over time) the study showed that the core areas of Operations, Watch and Warning, Analysis, Planning, Assist/Assess and Outreach provide an excellent set of domains for a SCADA cyber-threat and vulnerability management system. Perhaps more importantly, interaction with project partners and asset owners showed that these elements would (a) support effective information exchange between government and private sector, (b) help encourage private sector enrolment, and (c) create a management system that would dovetail into supporting cooperative incident response functions.

The study showed that requirements for a SCADA Threat and Vulnerability Management system must be viewed in the context of existing vulnerability management solutions. This was confirmed by project members and partners, and highlighted the approach to re-use process and technology to accommodate for the nuances associated with cyber security in the industrial automation domain. State of the art technical Vulnerability Management Solutions (VMS) are designed around the principle of continuous, differential vulnerability scanning and assessment, and this characteristic is required to ensure future-state approaches are sound. Information from different domains is aggregated from 'edges' to a central analysis function, which reports changes in the vulnerability environment to operators.

The key conclusion of this study is that the technology for a robust cyber vulnerability management solution exists, however the network of relationships required to implement it as a national infrastructure protection capability, as of yet, does not. Enterprise vulnerability management solutions must improve their ability to meet the needs and sensitivities of SCADA systems. In turn, SCADA system vendors must improve their software development lifecycle security so that they are at least as robust at off the shelf IT solutions.

The study showed that effective threat and vulnerability management systems are not dedicated solely to the understanding of the threats and vulnerabilities themselves, but rather they support how information is used to provide support for a proactive (protection) and reactive (recovery) lifecycle. In addition, the study showed that the best approach for a SCADA cyber threat and vulnerability management system incorporates features and characteristics of past management frameworks, and that certain aspects of traditional management frameworks can work well in future-state strategies. The key to a SCADA cyber threat and vulnerability management system is to find the pivot points for integration of the threat environment and technical vulnerability information.

In spite of its evident limitations, a 'clearing house' approach to vulnerability management in these sectors should be a part of the solution. Canada should establish a foundation for a network of stakeholders, which will provide a channel for education and for enrollment into their shared stewardship role in the security of national infrastructure. An exercise that determines the sectors, infrastructure, companies, organizations and contacts for national critical infrastructure in Canada would enumerate the constituency of stakeholders and illuminate further requirements for a clearing house capability to serve them.

The unique need implied by SCADA security is that an integration layer is required between critical infrastructure asset owners who already have access to vulnerability data, and the security agencies that can contextualize the data with current, strategic threat information. Clearinghouses have the capability to provide this layer since they may act as both a trusted proxy and an integrator for threat and vulnerability information.

The technical vulnerability management component will be a function of the maturity of IT security controls in the specific industry sector. The approach to SCADA system vulnerability by organizations surveyed as a part of this study conformed to first generation "Find and Fix" patterns. A next generation

solution would rely on find and fix approaches as well as state of the art enterprise vulnerability management and SEIM solutions to be functional in SCADA environments. Threat information from law enforcement and the IC could be filtered through clearing houses and provided to critical infrastructure asset owners, who would use it to filter information from their technical vulnerability management solutions. Asset owners could then share derivatives of the risk information, refined as a result of their own vulnerability information in the context of threats, with the clearing house for distribution to IC and law enforcement stakeholders.
The vulnerability of infrastructure in Canada would be reduced by the implementation of an approved SCADA solution products list similar to the Common Criteria "Certified Products" list.

Task 4 – Best Practice Security Guidance for SCADA Systems
The tasking in this project area was developed to provide a set of reasonable practices to Canadian critical infrastructure asset owners, for managing the security of their SCADA and control systems. It is intended that this work will enhance the resilience of Canada's critical infrastructure by providing recommended best security practices to asset owners. The tasking was completed following several key strategies:
Evaluate and leverage existing work done by the global community of interest and cross correlate with the findings and observables from previous study activities

Review functional security characteristics between SCADA and traditional IT strategies and incorporate stakeholder input into requirements to reflect Canadian interests.

The study team performed a comprehensive review of existing literature regarding SCADA security best practices and guidance, and incorporated feedback based on interactions with study partners and real-world assessment /training activities performed by the study team. The core activities of this task involved the establishment of a well-defined review committee of subject matter experts and partners who had specific interest and capability in the area of developing recommended practices and guidance for securing SCADA systems.
The study performed comprehensive review of existing literature specific to the tasking focus area, and included:
SCADA Assessment and GAP analysis with NIST SP-800 82 as core baseline standard
Smart Grid standards review and applicability analysis
Comprehensive review of findings and outputs from Study Tasks 1 and 2, and categorization of these findings as possible updates to existing work
Comprehensive reviews of existing recommended practices from DHS, CPNI, ISA, NIST,E-SCISE, AMI-SEC, NISTIR, AUS Attorney General, AGA, INGAA, DoT, U.S. TSA, API, NERC, and U.S. DoE

It is important to recognize, however, that the current landscape of best practices and security guidance for SCADA is rarely country specific, and that the current compendium of usable guidance presents Canadian asset owners a tremendous amount of choice when developing security strategies for their control systems.

Systems security management programs, as a concept, are not limited to IT environments. The security management program is a process which evaluates risks and selects controls to mitigate those risks. As a process, it can incorporate the special requirements of ICS environments and thus can be used to manage the security risks in ICS.
Currently, the volume of best practice security guidance available to SCADA and ICS asset owners is extensive. The ubiquity of security issues across the Canadian asset owner landscape allows for these practices to be applied across many sectors, while simultaneously addressing some of the unique challenges facing Canadian stakeholder. This study was able to assess the current state of available guidance and extract high-level direction that the Canadian asset owners can use to create effective SCADA resilience plans. This approach was discussed by study partners, and rather than simply re-create

existing guidance in a new format it was deemed more useful to prove insight to key overarching themes and supply a concise, well-researched set of references.
Based on the reviews of available best practiced and standards, combined with real-work experience demonstrated by the study team, the following high-level guidance can be provided to the Canadian community of interest. This guidance is to be considered complimentary to the granular direction provided in exiting literature and practices.
Assign a senior manager to be responsible for managing cyber security risks in ICS environments, and cross pollinate personnel between IT and SCADA on a regular basis.
Create a Security Management Program to assess and remediate risks with appropriate controls, accept residual risks, manage incidents, measure program success and perform self-improvement.
Identify every asset in the ICS environment and assign criticality to it. Establish its security assurance requirements based on an impact analysis, and use these results to shape processes for incident investigation and forensic activity.
Ensure a strong change management program is in place to reduce the risk that unauthorized or undocumented changes can occur to systems, applications and networks.
Create a comprehensive set of controls which match with security assurance (and system criticality requirements. Consider adopting a standard, if one is not already mandated by regulatory requirements, and make appropriate modifications to fit your environment.
Group systems with similar security requirements into access controlled network environments.
Ensure proper change management practices are observed so that administrators can be confident that they are aware of the state of the environment, including the state of security.
Provide dedicated systems for critical services and applications.
Harden systems and applications by removing extraneous functionality, improving authentication mechanisms, and improving access control enforcement, in accordance with the principle of least privilege.
Implement a robust incident management program, with resolution deadlines and the ability to evaluate and improve itself. This program should include robust anomaly detection mechanisms across environments, systems and applications.

5.2 Strategic advisory note

The primary objective of PSTP-02-347eSec "*Study on Cyber Security and Threat Evaluation in SCADA systems*" was to support the e-Security Community of Practice by leading a study to fill the knowledge gap concerning the current cyber-threat environment affecting SCADA systems. To ensure the study domain is appropriately positioned within the PSTP effort, analysis of the current project can facilitate for an excellent understanding of what issues require addressing as it pertains to enhancing the resilience of Canada's critical infrastructure. By addressing both enablers and barriers, the Community of Interest (COI) will be able to ensure value to the stakeholder community, and define future study requirements that can integrate with primary project objectives.
From the perspective of the overall PSTP mission, specifically regarding infrastructure protection, any study activity addressing the security of the actual technology running vital sector activities has clear value. However, the outputs from these studies must provide new information as opposed to the aggregation and rebranding of previously seen work. As the outputs from this SCADA security study has immediate applicability to stakeholders, either by recommended guidance or technology roadmaps, the PSTP must maintain an active interest in funding these efforts in a manner that focuses on the unique challenges of Canadian asset owners. This must be done in a manner that leverages work done by other countries and study activities.

PSTP can maximize their value by ensuring that the SCADA-related work efforts address how unique Canadian challenges are met. This is a non-trivial activity, as the problems stemming from the ubiquity of industrial automation and their security issues is global in nature Thus, Canadian stakeholders can seek and obtain useful and applicable SCADA security guidance from anywhere. The challenge for PSTP then becomes one of shaping the work scope of future SCADA security studies so that selected teams bring unparalleled leadership and technical capability, proven access to the Canadian stakeholder community, and a proven experience in global SCADA security activities (so as to reuse existing work in a manner that prevents unnecessary spending of research dollars).

Enablers to Facilitate Maximum Value to Stakeholders

Canada is a global leader in cyber-security. In that domain, Canada also has a small but exceptionally capable community of SCADA and industrial controls systems security subject matter experts. The current study was able to take advantage of the fact Lofty Perch, as the study leaders, is a globally recognized centre of excellence in SCADA/ICS security. Going forward, recognized technical and thought leadership from the Canadian SCADA security domain should be part of the COI. More importantly, these subject matter experts should be called upon to craft future calls for papers, be an integral part of the review process, and ensure the federal government partners are suitable project authorities. This will ensure that (a) PSTP SCADA security efforts provides the much-needed uniqueness that Canadian asset owners require for their resiliency activities, (b) budget allocations are being used in a manner that does not recreate already existing work, and (c) the government leadership have appropriate technical capability to interface between private sector study partners and public sector entities.

Another vital enabler that will increase the value to stakeholders is the recruitment of federal project leadership from organizations not traditionally to be PSTP technical authorities. To date, project positions held by the law enforcement community have proven very valuable, and the results from the SCADA studies do have results that can have immediate impact to the stakeholder community. With that, future study strategies that include project oversight from federal partners with mission activities specific to vital sectors can prove exceptionally beneficial. The sectors include, but certainly are not limited to, transportation, environmental, mining/minerals, and others that have a fairly granular area of responsibility. This suggestion translates directly as to how the results from technical research activities can be incorporated into critical infrastructure protection activities, with specific focus on sector-specific SCADA and control systems resiliency activities.

Barriers to Success and Appropriate Countermeasures

A research study requires that both project oversight and research activities are led by personnel who have the necessary technical background and experience to support a cyber-security research effort with an accelerated timeline and tempo. For PSTP, these requirements are mandatory to optimize the value proposition for the stakeholder community. The outputs of the research for SCADA projects within the PSTP effort should result in strategic and tactical guidance that can be used by the stakeholders to create more effective resiliency strategies for their industrial automation environments. The importance of public/private collaboration cannot be overstated, and a strong capability to transfer research findings to asset owners is just as important as the capability to include stakeholder concerns and ideas into the research process. As such, the ability for the PSTP project technical authority and study leadership to create and execute upon a fluid process that ensures rich technical accuracy in project activities is critical to project success. Upon review, it is recommended that PSTP COI consider federal government involvement (from a technical authority perspective) be reviewed to ensure technical subject matter expertise is integrated into the oversight function. Not only will this ensure that the interpretation of study findings can be understood and disseminated to the appropriate stakeholders, but will improve the applicability of information products and reduce the time required to provide feedback to the study team. Regarding in-kind support, PSTP could benefit from a better process as it relates to the development of contingency planning for loss in-kind support during the project lifecycle. In many cases, the elapsed time from study award to contract completion is considerable and results in many study partners having to withdraw their support. The reasons for this can be many and include budget constraints, changes in investment focus, or partner contacts becoming unavailable. Access to stakeholders may also be impacted due to the ever-changing workload federal partners are subject to, and demands of these partners may

make access to other federal study peers impossible. Regardless of the reasoning, successful study completion may become highly dependent on the personal relationships that the study research team maintains. To help mitigate this problem, it is recommended that PSTP COI review the nuances associated with the SCADA security and critical infrastructure community and proactively determine a strategy to assess whether or not the proposed mitigation strategy (addressing changing in-kind support levels) is truly appropriate.

From a strategic perspective, the overall value proposition of the PSTP is significantly enhanced with the inclusion of research specific to the security of SCADA and industrial automation. It is very clear that the outputs from these studies have immediate applicability to the security posture of the Canadian national critical infrastructure and have outputs that can cross pollinate research activities that in other domains of interest. The recently completed study showcases several areas that can improve the overall programmatic strategy, all of which leverage successes that the program has seen to date. The SCADA security technical capabilities within the Canadian private sector, combined with the overwhelming interest by the stakeholder community, create a landscape upon which the results from the studies can easily be disseminated. Future state programs will be able to leverage these factors by ensuring the outputs from the research are tuned to accommodate the specific needs of individual sectors. Although the overall program objectives and goals can remain the same, PSTP should look to refine the review process to ensure mitigation strategies for risk remediation are appropriate, and extend the programmatic community of interest to include federal government parties that may be more adept at transferring information products into sector-specific requirements.

5.3 Capabilities road map

In reviewing the objectives and scope of the "*Study on Cyber Security and Threat Evaluation in SCADA Systems"*, and taking into consideration the advice provided in the project Strategic Advisory Note (SAN), a Capability Road Map (CRM) can be developed to ensure continued success for the PSTP activities focusing on SCADA security. The completion of the current study provides an excellent opportunity to review project enablers and barriers, and provide insight to what improvements can be made within the study life cycle support domains. This CRM has been developed by the current study team to provide a commentary on the elements required to ensure success of the PSTP study programs addressing SCADA and industrial control systems security. More importantly, this CRM discusses future areas of focus that have been designated out of scope for the current study and takes into consideration activities that have occurred in the community of interest over the last year. This is a sound approach, as addressing these items within the current study lifecycle would have prohibited the project from maintaining alignment with study goals and would not have facilitated for the project being able to finish well under budget.

Several issues can contribute to the success of study programs involving SCADA and industrial control system cyber-security. The completion of the current study indicated that these issues, if unmitigated, could have a negative impact on the overall study success. For the current study, the consequence of these issues was minimized due to the extensive technical experience of the study team and the stakeholder community access maintained by the study team. To ensure such issues do not impede future study teams, this CRM has been developed making the following assumptions and leverages the positive mitigation activities demonstrated in the past study:

There is no significant delay in time between selection of study team and completion of contract, thus empowering the study team to begin executing on the proposed study lifecycle and research activities as soon as possible

The extent of in-kind support capability is manageable and there is a definitive contingency plan to compensate for any loss of proposed in-kind support

The guidance from this Road Map will provide direction as to how Science and Technology (S&T) will maintain a capability to provide strategic advice on SCADA security. As cited in the Strategic Advisory Note, Canadian asset owners and stakeholders have a wide range of accessible resources to help the proactive and reactive protection strategies for critical infrastructure industrial systems. The challenge for future studies becomes one of ensuring that existing information is reused appropriately, and that new research results and information accommodate for sector specific needs that are uniquely Canadian. Clearly, the infusion of private sector subject matter expertise into the study scope will be required. Private sector SCADA security expertise is needed in the review process to ensure the applicability of those information products created by the studies. The inclusion of unbiased private sector subject matter experts to expedite enrolment from the Canadian asset owner community, while at the same time ensuring that funding is directed to programs that can advance the work of previous studies, is critical to success. An analysis of the work plan for the *Study on Cyber Security and Threat Evaluation in SCADA Systems* showcases an ideal set of activities dispersed over the course of a year, and defines an excellent foundation for the strategy that can be adhered to in studies.

To ensure these future studies build on pre-existing work, and that the outputs from future PSTP SCADA security studies provide tangible guidance for asset owners, the roadmap must be sensitive to incorporating the 'wants and needs' of critical infrastructure sector representation and cross-correlate those needs with available (and proven) security technology. It is expected that each future study will build on the outputs from its predecessor, and that with each new study activity there is tasking that seeks to obtain results that are more granular than those observed in previous projects. As has been shown, these outputs must also be made available to those federal agencies (law enforcement and intelligence) responsible for the outreach programs involving critical infrastructure entities. As many of the recommendations are often very technical in nature, it is recommended that those federal entities involved in collaborative efforts with private stakeholders have the necessary technical understanding of background research to empower asset owners to deploy useful security countermeasures. These requirements should be embedded in the study lifecycle as a maintenance or human resources activity, and the persistence of this function in each study will facilitate for the capability to measure the effectiveness of study results year after year.

A PSTP research study requires that both project oversight and research activities are led by personnel who have the technical background and experience to support a cyber-security research effort with an accelerated timeline and tempo. For PSTP, these requirements are mandatory to optimize the value proposition for the stakeholder community. The outputs of the research for SCADA projects within the PSTP effort should result in strategic and tactical guidance that can be used by the stakeholders to create more effective resiliency strategies for their industrial automation environments. The importance of public/private collaboration cannot be overstated, and a strong capability to transfer research findings to asset owners is just as important as the capability to include stakeholder concerns and ideas into the research process. The ability for PSTP project technical authority and study leadership to create and execute upon a fluid process that ensures rich technical accuracy in project activities is critical to project success. Upon review, it is recommended that PSTP COI consider federal government involvement (from a technical authority perspective) be reviewed to ensure technical subject matter expertise is integrated into the oversight function. Not only will this ensure that the interpretation of study findings can be understood and disseminated to the appropriate stakeholders, but will improve the applicability of information products and reduce the time required to provide feedback to the study team.

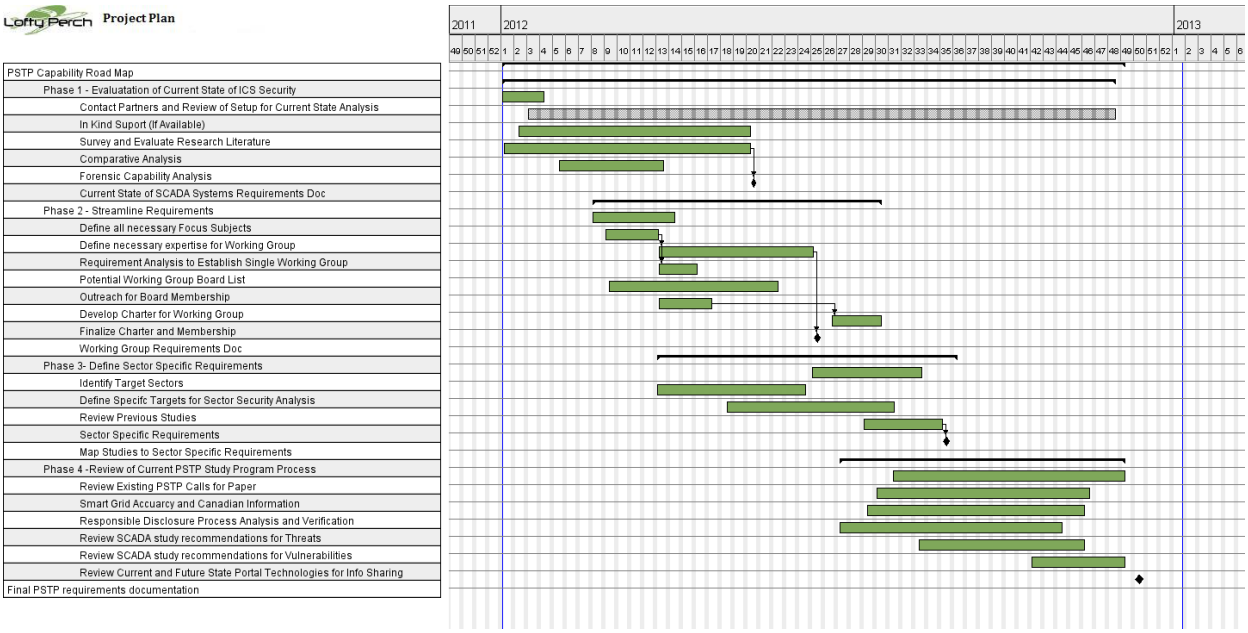
Regarding in-kind support, PSTP could benefit from a better process as it relates to the development of contingency planning for loss of in-kind support during the project lifecycle. In many cases, the elapsed time from study award to contract completion is considerable and can result in study partners having to withdraw their support. The reasons for this can be many and include budget constraints, changes in investment focus, and partner contacts becoming unavailable. Access to stakeholders may also be impacted due to the ever-changing workload to which the federal partners are subject to Demands of these partners may make access to other federal study peers impossible or difficult. Successful study completion may become highly dependent on the personal relationships that the study research team

maintains. To help mitigate this problem, it is recommended that PSTP COI review the nuances associated with the SCADA security and critical infrastructure community and proactively determine a strategy to assess whether or not the proposed mitigation strategy (addressing changing in-kind support levels) is truly appropriate.

Notable Project Gaps and Out-of-Scope Elements Requiring Consideration:

An analysis of how contemporary cyber-security research techniques and procedures map to the industrial automation domain is required
Streamline the requirements for the development of project 'working groups', as the establishment of a working group for each and every task can incur unnecessary cost. Project scoping should define a single advisory working group populated with the necessary expertise to ensure successful study
Include sector-specific security requirements analysis, with specific attention to how the SCADA security solutions reviewed in previous studies map to sector-specific requirements
Consider including a review and assessment of how a responsible and coordinated disclosure process can increase the effectiveness of information sharing within the Canadian SCADA community of interest
Review and update existing PSTP calls for papers to ensure verbiage regarding Smart Grid studies is timely, accurate, and guarantees new information for Canadian asset owners
Advance the SCADA study activities pertaining to information sharing, with specific focus on the development of portal technologies that can be used to solicit intelligence from the asset owner community and provide a secure pathway for the dissemination of threat and vulnerability information

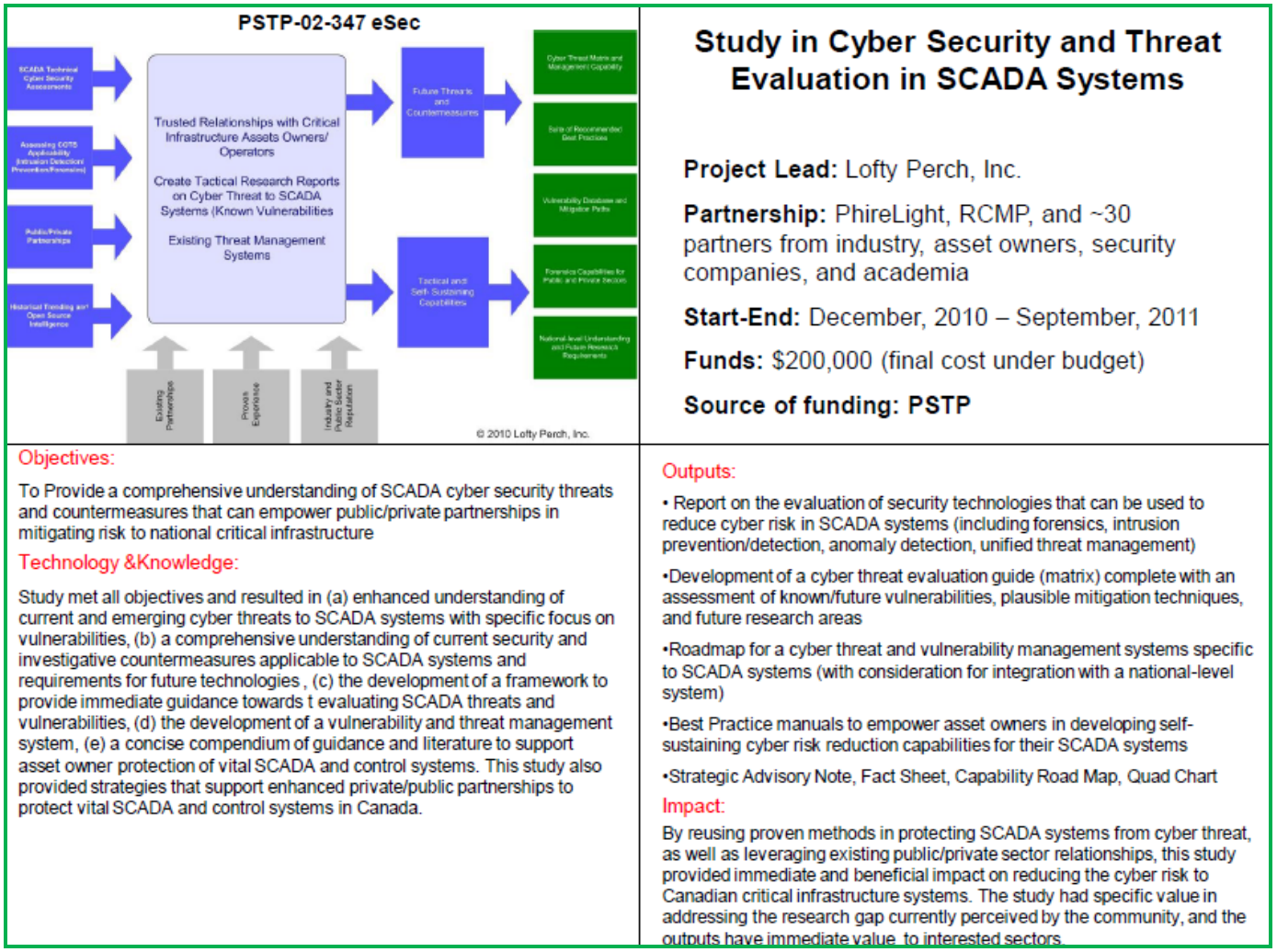
To help the PSTP effort deliver continuous value to the Canadian critical infrastructure community, a concise Gantt chart has been developed to outline the necessary study activities over a 6 month period that need to be addressed to support the lifecycle of a SCADA security project.



5.4 Study fact sheet

Project Overview/Objective: Support the e-Security Community of Practice by leading a study to fill the knowledge gap concerning the current cyber-threat environment affecting SCADA systems. This work is intended to enhance the resilience of Canada's critical infrastructure by providing direction to research and development programs and recommending best security practices. This primary objective is supported by the following complementary objectives:
To establish trusted relationships with private sector critical infrastructure SCADA operators;
To enable the production of research reports on the current cyber-threat environment to SCADA systems;
To contribute to the development of a cyber-threat management system for continued situational awareness; and
To contribute to the development of best practices for the security of SCADA systems.
Project Lead: Lofty Perch, Inc.
Federal Partners: Royal Canadian Mounted Police
Industry Partners: Phirelight e-Business Solutions
Authors: Mark Fabro, Lofty Perch, (905) 489-2827, fabro@loftyperch.com
Results: Overall, all of the primary and supporting study objectives were met. Focusing on four key areas of research, the study resulted in detailed information products providing (1) a comprehensive understanding of how contemporary commercial security products can accommodate for unique intrusion detection and forensic requirements in SCADA environments, (2) interpretation and analysis of the cyber-vulnerability landscape directly applicable to SCADA domains (complete with cross correlation of perceived threats), (3) a foundational framework for the scope and capabilities of a threat/vulnerability management system for SCADA systems, and (4) a SCADA security best practice manual, one that leverages pre-existing research and accommodates for unique Canadian stakeholder requirements.
The work scope developed for the study facilitated for numerous activities to be done simultaneously, and extensive stakeholder collaboration activities were performed to ensure final products were timely and useful. The study team used its access to the stakeholder community and incorporated real world cyber incident investigation results directly into research activities, and these results are aggregated with the extensive technical research that was performed in a laboratory environment. The project was continuously sensitive to ensuring that previously completed work was utilized, such as using standardized threat and risk assessment frameworks, and that new information was appropriately presented and integrated into the findings. This approach ensured stakeholder and project partner interests were addressed, and that in-kind partner contribution was maximized. The project was completed under budget.
The resulting information products provided comprehensive guidance, both technical and non-technical, that can be leveraged by the Canadian critical infrastructure asset owners in enhancing their efforts to develop resilient SCADA and control systems and facilitate for federal entities to better understand how to support critical infrastructure asset owners in proactive and reactive SCADA security activities.

5.5 Final project quad chart



DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Lofty Perch, Inc.
15-505 Hood Road
Markham, ON
L3R 5V6

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Study on Cyber Security and Threat Evaluation in SCADA Systems:

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Fabro, Marc

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
March 2012	171	92

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
PSTP 02-347eSec	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS CR 2012-006	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Le présent rapport fait la synthèse des résultats du projet PTSP 02-0347eSec intitulé Étude en cybersécurité et en évaluation des menaces pour les systèmes SCADA. L'objectif principal des responsables du projet est d'appuyer la communauté de praticiens de la sécurité électronique par la réalisation d'une étude scientifique qui vise à combler les lacunes dans les connaissances sur l'environnement de cybermenace actuel qui affecte les systèmes d'acquisition et de contrôle des données (SCADA). Ces travaux ont pour but d'accroître la résilience des infrastructures essentielles canadiennes en fournissant une orientation aux programmes de recherche et de développement et en recommandant des pratiques exemplaires en matière de sécurité. Cet objectif principal se divise en objectifs complémentaires de la façon suivante :

1. établir des relations de confiance avec les opérateurs SCADA des infrastructures essentielles du secteur privé;
2. permettre la production de rapports de recherche sur l'environnement de cybermenace actuel qui affecte les systèmes SCADA;
3. contribuer à l'élaboration d'un système de gestion des cybermenaces qui favorise une connaissance constante de la situation;
4. contribuer à l'élaboration de pratiques exemplaires pour la sécurité des systèmes SCADA.

Le rapport se divise cinq parties :

1. Tâche 1 : « Évaluer ce qui se fait de mieux en matière de cybersécurité des systèmes SCADA »
2. Tâche 2 : « Élaboration de lignes directrices en matière d'évaluation de la cybermenace et de la vulnérabilité »
3. Tâche 3 : « Définir la portée et les capacités d'un système de gestion de la cybermenace et de la vulnérabilité »
4. Tâche 4 : « Rédiger un guide ou un manuel des pratiques exemplaires en matière de sécurité »
5. Conclusions finales, note de consultation stratégique, feuille de route des capacités, fiche d'information relative à l'étude et tableau à quatre volets

Sommaire

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

SCADA; Threat Evaluations; Control Systems; Power